Privacy Impact Assessment
for the

TSA Claims Management System

February 5, 2007

Contact Point
Nicholas Panuzio
Director, Claims Management Office
Transportation Security Administration
(571) 227-1983

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 Department of Homeland Security (DHS) Transportation Administration (TSA) has created the Claims Management System (CMS). The TSA Claims Management Office (CMO) investigates and adjudicates Federal tort claims filed against TSA. The CMO developed the CMS as the primary tool for the CMO to receive, investigate, and adjudicate Federal tort claims against the Transportation Security Administration. This PIA covers all claims submission processes.

Introduction

The TSA Claims Management Office (CMO) currently receives and adjudicates numerous claims per month arising from airport screening activities and other circumstances, including motor vehicle accidents and employee loss. TSA currently receives claims by facsimile, U.S. mail, or other means.

In order to increase the effectiveness of the claims program, the CMO has developed the CMS as the primary tool to receive, investigate, and adjudicate Federal tort claims against the Transportation Security Administration. The Director of the CMO maintains and administers all claims against TSA. Submission of a claim is entirely voluntary and initiated by claimants. Claimants file a claim by submitting to TSA a Standard Form 95 (SF 95), Claim for Damage, Injury, or Death, a form prescribed by the Department of Justice, or other written submission containing information required to file a legally sufficient claim under the Federal Tort Claims Act (FTCA). In addition to the SF 95, TSA will ask claimants to complete a Supplemental Information form, which is agency specific to TSA. Any information concerning violations or potential violations of law or regulation may be shared within DHS and with the appropriate Federal, state, or local law enforcement agencies. TSA may also share claim information with U.S. Department of Justice (DOJ) for the purpose of representing the U.S. Government in tort litigation or for approving an administrative claim payment in an amount over $50,000.00. If, after review of these two forms, TSA determines payment is warranted, TSA will send the claimant a third form requesting the claimant's Social Security Number (SSN) or other taxpayer identification number and banking information in order to direct payment to the claimant. TSA will provide the U.S. Coast Guard Financial Center (CGFC) with the claimant's name, address, SSN, and banking information for the purpose of compensating claimants.

TSA has developed CMS, which is an online claim submission system by which claimants may submit claims electronically. The online system streamlines the information collection so that claimants can input all the necessary information in one location and ensure claims are completed sufficiently the first time. The system allows the claimant to check the status of the claim by entering a control number assigned to the claim. The online system will also increase TSA's efficiency in processing claims. CMS also allows TSA to identify trend data for conducting investigations into potential theft, locating possible victims of theft, or investigating potential fraudulent claims.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

TSA will collect the following information from claimants: name, signature, address, phone number, email address, flight information, airport location, air carrier information, dates/times of incident, details of the incident, demand for sum certain, and receipts, substantiation and appraisals. The Federal Tort Claims Act (FTCA) requires a claimant's name, signature, demand for sum certain, and

incident information in order to file a legally sufficient claim.

After investigation, should TSA determine that payment is warranted, TSA will provide the claimant with a payment form, which requests the claimant's signature, banking information (routing and account numbers required by the U.S. Treasury for all Federal payments pursuant to 31 U.S.C. §3332), and SSN (required by the U.S. Treasury for all Government payments to the public pursuant to 31 U.S.C. §3325). TSA currently maintains a paper copy of the payment form.

1.2 From whom is information collected?

This information is collected from any individual who files a claim with TSA for a loss due to the alleged negligent or wrongful act or omission of TSA or its employees.

1.3 Why is the information being collected?

This information is being collected in order to investigate and analyze tort claims filed against the agency to determine alleged TSA liability and to reimburse claimants when payment is warranted. In some cases, the information may be used to identify victims of theft or to further the criminal investigations into property theft.

1.4 How is the information collected?

The information is collected directly from the individual on the claims forms when they are submitted. If reimbursement is required, then the additional information is requested from the claimant on a payment form.

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

Under the Federal Tort Claims Act (FTCA) 28 U.S.C. §§ 1346(b), 1402(b), 2401(b), 2671-2680, and implementing regulations issued by the U.S. Department of Justice at 28 C.F.R. part 14, a legally sufficient claim must include the claimant's signature, a statement for sum certain (specific amount of money claimed), and a description of the incident sufficient to permit TSA to investigate. This includes the location and date of the incident. The collection of a SSN when payment is warranted is required by the U.S. Treasury for all Government payments to the public pursuant to 31 U.S.C. §3325. Collection of one's banking information when payment is warranted is required by the U.S. Treasury for all Federal payments pursuant to 31 U.S.C. §3332.

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.

TSA is collecting information necessary to complete an investigation into claims presented by the public and facilitate payment when warranted. Personally identifying information, such as name, address, email address, and phone number, is collected to facilitate communications with the individual. SSN and banking data are only collected when there is a determination to pay the individual and is mandated by law. Therefore, TSA is collecting the minimum information necessary in order to make a claim determination.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

The information is used to investigate the claim and to facilitate payment of the claim when warranted. Information concerning the details of the specific incident is also used to identify trend data at particular airports for the purpose of conducting investigations into potential theft. When TSA determines payment is warranted. TSA collects a claimant's SSN, that information is used by the U.S. Treasury in order to facilitate all Government payments to the public pursuant to 31 U.S.C. §3325. When payment is warranted, TSA also collects banking information pursuant to 31 U.S.C. §3332.

The information is also used by the TSA Office of Inspection (OI) when investigating TSA employees or other airport/airline employees for possible theft, for locating possible victims of theft, or for investigating potentially fraudulent claims. Any information concerning violations or potential violations of law or regulation may be shared within DHS and with the appropriate Federal, state, or local law enforcement agencies in accordance with the routine uses identified in the applicable Privacy Act System of Records Notices (SORNs), DHS/TSA 006, Correspondence and Matters Tracking Records and DHS/TSA 009, General Legal Records. Both SORNs were published in the Federal Register on August 18, 2003, and can be found at 68 Fed. Reg. 49496, 49503, and 49503.

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

The incident data, and in some cases personally identifiable information, is used to identify victims of theft and track any trends regarding missing items and other trends in an effort to reduce claims and to notify TSA Federal Security Directors when possible problem trends are identified. It may also be used to identify possibly fraudulent claims.

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

The information will be provided by the applicant either by mailing the necessary forms or, when the online system is operational, by submitting data directly online. For manual submission, after TSA enters a claimant's data, the data is subject to a quality assurance process, which is comprised of a visual check of the claim form against the data entered into the CMS. All personal contact information and the details concerning the nature of the claim are confirmed with the claimant during the investigative process.

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 CMS is password-protected and only those TSA employees who have a need to access the system in order to perform their official duties are granted access to the system. All CMO employees have completed a TSA online privacy training course. All of these efforts are made to ensure that information

contained in the CMS is used in accordance with the Privacy Act and applicable DHS and TSA privacy regulations and policies.

Section 3.0 Retention

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

CMS records that include correspondence and other documents, including documentation related to incidents for which a prospective claimant does not submit a sufficient tort claim, will be retained for three years. CMS records relating to claims against the United States, which includes documentation related to tort claims for monies that TSA has allowed or disallowed, once inactive, will be retained for six years.

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

Yes. The CMO currently has an approved retention schedule from NARA (TSA 600.9).

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

The retention of this information for the specified retention period is the minimum required to address any potential disputes or litigation which may arise after the claim is processed.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

In the ordinary course, information will be retained and used within CMO, but also will be shared with other TSA authorized users, including the TSA Office of Chief Counsel, TSA personnel responsible for customer service and stakeholder relations, and the TSA OI. Further, the information TSA receives from claimants may be shared with DHS employees and contractors who have a need for the record in the performance of their duties, including but not limited to CGFC for the purpose of compensating claimants.

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

The claim information will be shared with the Office of Chief Counsel for legal review of claims. The claim information may be shared with TSA personnel responsible for customer service relations and incident follow up. The information may also be shared with the TSA OI to investigate TSA employees or other airport/airline employees for possible theft, for locating possible victims of theft, or for investigating potentially fraudulent claims. TSA will provide CGFC with the claimant's name, address, SSN, and banking information for the purpose of compensating claimants. 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?

On a day-to-day basis, claim information may be transmitted within TSA via paper file, electronic means, or via access to the CMS database by authorized users. Electronic payment requests are received via facsimile in a secured office within TSA Headquarters. They are stored in the locked office or within a locked file cabinet at all times. Additionally, the entire floor is accessible by TSA employees during business hours and has limited access after hours. Only the CMO Director, CMO Finance Analysts, and Office of Chief Counsel have access to the payment data.

Electronic payment requests are then transmitted to CGFC via two secure means. The flat-file text format is transmitted via secure FTP and the backup Excel spreadsheet is transmitted within a password-protected and encrypted zip file. The flat-file is then imported into the CGFC finance systems and compared to the Excel spreadsheet. For foreign payments and payment requests for electronic fund transfer (EFT), copies of claim source documents are sent to CGFC via express shipment contractor. Payment information for these claims is entered manually by CGFC.

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

Authorized CMS users are limited to the those individuals who have a need to access the information to perform their official duties, including the CMO Director and CMO staff, certain TSA staff responsible for customer service and stakeholder relations, personnel from the Office of Chief Counsel, and personnel from the TSA OI. The electronic payment forms are stored and secured in accordance to instructions supplied by the TSA OI. Access to the payment information is limited to the CMO Director, CMO Finance Analysts, and the Office of Chief Counsel. The information transmitted to CGFC includes only the data necessary for payment to the claimant. To mitigate potential privacy concerns, TSA has carefully determined the structure and content of the data necessary to be transmitted to CGFC in order to pay claimants.

Section 5.0 External sharing and disclosure

5.1 With which external organizations is the information shared?

TSA shares claimant information with Financial Management Service, U.S. Department of Treasury (FMS) when a payment is to be made, and with the DOJ if a case is initiated. Aside from FMS and DOJ, TSA may also share the information it receives in accordance with the routine uses in the applicable Privacy Act system of records notices (SORNs), DHS/TSA 006, Correspondence and Matters Tracking Records, and DHS/TSA 009, General Legal Records.

5.2 What information is shared and for what purpose?

TSA shares claimant information with FMS for the purpose of compensating claimants in an amount over $2,500. TSA may also share claim information with DOJ for the purpose of representing the U.S. Government in tort litigation, or for approving an administrative claim payment in an amount over $50,000.00. Aside from FMS and DOJ, TSA may also share the information it receives in accordance with

the routine uses in the applicable Privacy Act system of records notices (SORNs), DHS/TSA 006, Correspondence and Matters Tracking Records, and DHS/TSA 009, General Legal Records.

5.3 How is the information transmitted or disclosed?

TSA may transmit claim information in person, via email, facsimile, or telephone. Claim payment information is forwarded to FMS via express shipment contractor. CMS encrypts claims information when sent office site and as such complies with OMB Memo 06-16. The CMS website has encryption.

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?

No. The Privacy Act System of Records Notices described above provides the necessary allowances for sharing of the information.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act and their applicable SORNs, and to the extent the information is maintained electronically, consistent with Federal Information Security Management Act (FISMA).

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

No specific training is required by TSA. Federal agency employees typically are required to undergo Privacy Act training by their employing agencies.

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

The information transmitted to FMS includes only the data necessary as required by FMS for payment to the claimant. TSA may also share this information under the applicable provisions of the SORNs and the Privacy Act. By limiting the sharing of this information and by ensuring that recipients properly handle this data, TSA is mitigating any attendant privacy risks.

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?

A Privacy Act Statement is provided to claimants on the SF 95, the supplemental questionnaire, and the payment form. A Privacy Act Statement will also be provided to claimants on the online claim submission system. In addition, individuals may learn about the system by consulting the applicable system of records notices (SORNs), DHS/TSA 006, Correspondence and Matters Tracking Records, and DHS/TSA 009, General Legal Records

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

Claimants always have a right to refuse to provide information. The CMO advises the claimants that their claim will be adjudicated with the information provided. However, if the information a claimant provides does not meet legal sufficiency requirements, TSA may not be able to process the claim.

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.

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

TSA will collect only that information regarding the claim that is necessary to investigate and process the claim. If a claimant refuses to provide information, the CMO will adjudicate the claim based on the information provided by the claimant. It is in the best interest of the claimant to provide as much detail as possible in order to facilitate the processing of their claim. Claimants are provided with meaningful notice that enables them to exercise informed consent prior to disclosing any information to TSA, and always have the right to refuse to provide information.

Section 7.0 Individual Access, Redress and Correction

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

Claimants may contact TSA to correct or make changes to their own information after submitting a claim to TSA. For claims submitted online, claimants will be able to contact TSA with updates and additional information.

In addition, 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 Act Office, TSA-20

11th Floor, East Tower

601 South 12th Street

Arlington, VA 22202-4220

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

7.2 What are the procedures for correcting erroneous information?

The TSA Contact Center or CMO will correct any erroneous claims information contained in the database immediately upon request by the claimant.

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

TSA will inform claimants if their information is not complete or inaccurate. In addition, claimants are provided a toll free telephone number for the TSA Contact Center for inquiries or any other questions related to their claim.

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

Claimants may contact TSA to correct or make changes to their own information after submitting a claim to TSA. For claims submitted online, claimants will be able to contact TSA with updates and additional information.

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 CMO will correct and update claimant information as this may assist the CMO in adjudicating the claim. Individuals may request access to or correction of their personal information by contacting the TSA CMO and pursuant to the Freedom of Information Act and Privacy Act. TSA expects that information submitted by the individual will be accurate since it is submitted under oath by the individual.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

In order to perform their duties in managing, upgrading, and using the system, system administrators, delegated authority officials, claim examiners, administrative personnel, TSA customer service and stakeholder relations personnel, and counsel have access to the CMS. Further, personnel from the TSA Office of Inspection may have access to the information in CMS for purposes of investigating TSA employees or other airport/airline employees for possible theft, for locating possible victims of theft, or for investigating potentially fraudulent claims. No unauthorized users are permitted access to system resources. The public may access the web interface module of the overall CMS at http://www.tsaclaims.org. Online, individuals may check the status of their own claim only. Once the online system is implemented, claimants may file a claim electronically

8.2 Will contractors to DHS have access to the system?

Yes, CMO contractors who are hired to perform many of the IT maintenance and security monitoring tasks will have access to the system.

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

Yes. The privileges range from "read only" to "Administrator." The Administrator has the right to change any data within the CMS.

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

The Director of the CMO is also the primary Administrator for the application. The Director determines the access required by the user based on the individual's need to access this information to perform an official function.

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

Assignments of roles and rules are hard-coded into the CMS programming. The CMS software that controls the assignments of roles and the levels of access is reviewed on an annual basis in accordance with the CMS System Security Plan (SSP). The SSP describes in detail all measures taken to ensure the CMS complies with Government IT standards as dictated by the FISMA. Additionally, all access attempts are logged on the CMS server for audit purposes.

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

The CMS IT SSP describes the auditing measures and technical safeguards in place to prevent misuse of data. For example, as outlined in the SSP, a server intrusion detection system (SIDS) and network intrusion detection system (NIDS) automatically and constantly monitor all login traffic. Also, the system automatically undergoes penetration testing, to monitor any attempt to hack into the system. The TSA Chief Information Officer (CIO) approved this plan and granted the Authority to Operate (ATO) on August 15, 2006. Under this plan, the CMS will be audited annually for IT security policy compliance and technical vulnerabilities by the TSA IT Security Office.

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

Training is provided internally by the CMO Management. In addition, all government and contractor personnel are required to complete the on-line TSA Privacy Training Compliance with this requirement is audited monthly by the TSA Privacy Office.

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

Yes. The CMS is a Certified and Accredited IT system. The CMS was certified and accredited and granted the ATO by the TSA CIO on August 15, 2006 for three years.

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 will be secured in accordance with applicable Federal standards. By complying with the policies and procedures of the TSA IT Security Office, the CMS will continue to receive the attention required to ensure the safeguarding of the CMS data.

Section 9.0 Technology

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

The CMS was built from the ground up.

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

Data integrity, privacy, and security were a vital part of the system design in the following ways. By utilizing a role-based system, only authorized personnel with a valid need to know have access to the claim personal data. All hardware systems and software were built to protect the data from improper access and to comply with FISMA and all other applicable security and privacy policies mandated for Federal IT systems. For example, as outlined in the SSP, a server intrusion detection system (SIDS) and network intrusion detection system (NIDS) automatically and constantly monitor all login traffic. Also,

the system automatically undergoes penetration testing, which determines whether anyone attempts to hack into the system.

9.3 What design choices were made to enhance privacy?

The following design choices were made and rules were employed to enhance security of the information and the system:

- The web interface on which the individuals can check the status of their claims was placed on a separate server with a private connection to the application server. This protects the application server and data from unauthorized access.
- Releasing information to claimant family members or another third party requires written authorization from the claimant.
- Claimants that contact the CMO with a claim number must provide other means of identification before any claim information is released. Telephonically, this includes verification of their address, phone number, email address, incident date, etc.
- Claimants who access the web site for claim status can only enter their claim number and receive the claim status. No other information is provided.
- Paper copies of claims which include claimant SSNs and banking information, are secured in a locked office and locked filing cabinet. This office also maintains a dedicated FAX machine that receives after-hour faxes, including claims information, within the locked office. Access to this office after normal business hours is limited to the CMO Financial Manager, the CMO Director, and TSA Security.
- Electronic copies of the claims are protected by a user name and password system.
- The Claims Office floor is accessible during business hours to TSA employees and with limited access after hours. All SSNs and banking information are kept in a locked file cabinet at all times. TSA does not store claimants' SSNs or banking information electronically.
- Prior to receiving ATO for CMS, the CMO hired a professional IT Security Firm to assess and audit every aspect of the system.

Conclusion

The overall CMS system was designed from the outset to be reliable and secure. Data integrity was a priority when choosing the application platform, backup systems, software design, etc. Further, the security of the system continues to be a priority. The CMO hired a professional IT Security Firm to assess and audit every aspect of the system, and TSA IT security personnel will audit the system on an annual basis in accordance with the System Security Plan. TSA respects the privacy of claimant information and strives daily to ensure the data remains secure.

Responsible Officials

Nicholas Panuzio
Director, Claims Management Office
Transportation Security Administration
Department of Homeland Security

Approval Signature

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

_____

Hugo Teufel, III
Chief Privacy Officer
U.S. Department of Homeland Security