Privacy Impact Assessment
for the

Claims Management System

DHS/TSA/PIA-009(a)

May 1, 2019

Contact Point
Sherry Johnson
Claims Branch Manager
Transportation Security Administration
TSAClaimsOffice@tsa.dhs.gov

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration's (TSA) Claims, Outreach, and Debt Branch (COBD) investigates and adjudicates claims against TSA involving property loss or damage.[1] TSA uses the Claims Management System (CMS) to process these types of claims. As such, CMS collects Personally Identifiable Information (PII) from members of the public and TSA personnel. In accordance with Section 208 of the e-Government Act of 2002, TSA is conducting a new Privacy Impact Assessment (PIA) to reflect current procedures and replace the CMS PIA originally published in 2007.[2]

Overview

TSA is responsible for securing of all modes of transportation.[3] Pursuant to this authority TSA screens all aviation passengers and their baggage[4] before granting access to the airport's sterile area.[5] When a passenger experiences a loss of or damage to his or her personal property or suffers a personal injury and feels this occurred as a result of TSA negligence, the passenger or property owner may file a claim with TSA seeking compensation under the Federal Tort Claims Act (FTCA).[6] TSA employees may file a claim with TSA for loss of or damage to personal property incident to service under the Military Personnel and Civilian Employees' Claims Act (MPCECA).[7]

TSA receives approximately 10,000 claims a year from the traveling public and TSA personnel, typically for issues arising out of airport screening activities. In order to facilitate efficient processing of claims, TSA developed an automated case management database called CMS. CMS is used to intake, process, analyze, and track claims; thus, it maintains PII submitted in connection with claim packages.

Claims filed under the FTCA must be submitted to TSA in writing within two years of the incident and must state the specific date, location, and circumstances of the loss or damage, and a demand for money damages in a sum certain for injury to or loss of property. The claim must also be signed by the claimant or the claimant's authorized representative. TSA encourages individuals to use TSA's Tort Claim Package, which includes a Standard Form (SF) 95, *Claim for Damage,*

[1] TSA's Chief Counsel investigates and adjudicates claims involving injury to or loss of property, personal injury, or death.
[2] *See* DHS/TSA/PIA-009 Claims Management System (CMS) (February 5, 2007), *available at* https://www.dhs.gov/privacy.
[3] 49 U.S.C. § 114.
[4] 49 U.S.C. § 114(e)(1).
[5] "Sterile area" means a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier through the screening of persons and property. 49 C.F.R. Part 1540.5.
[6] 28 C.F.R. Part 14.3.
[7] 31 U.S.C. 3721.

Injury or Death, SF 95 instructions, and a SF 95 *Supplemental Information* sheet that collects specific information about the individual's travel itinerary. TSA will, however, accept a claim in any written form that contains the following required information: a statement of the claim sufficient to give the agency notice to investigate; a demand for a sum certain; and the signature of the claimant or the claimant's authorized representative.

The SF 95 collects the minimum amount of information needed for a claims examiner to promptly initiate and thoroughly conduct an investigation into the claim. The SF 95 also helps to reduce the time required to fully process the claim. The claimant must sign the SF 95 to acknowledge civil and criminal penalties for presenting a fraudulent claim or making false statements. The package can be downloaded from TSA's Claims website at https://www.tsa.gov/travel/passenger-support/claims.

For claims filed under MPCECA, TSA employees may use Form DD-1842, *Claim for Loss of or Damage to Personal Property Incident to Service* and Form DD-1844, *List of Property*, if necessary. The claim form must be signed by the employee. MPCECA claims must be filed within two years after the employee discovers, or should have discovered, the loss or damage. The claim must also include a statement from the employee's supervisor certifying that the employee was in a duty status at the time the claim arose and providing any additional information about the validity of the claim that he or she may have.

Once received, TSA uploads the claim into CMS and sends the claimant an acknowledgement letter with a control number. The claimant can use the control number to check the status of his or her claim online at https://apps.tsa.dhs.gov/cmsstatus/. In CMS, the claims examiner reviews the claim for legal sufficiency. A claim is deemed legally sufficient if it is filed within two years of the incident and includes all of the following: the specific date of the loss or property damage; the location of the incident; the circumstances of the loss or damage to property; a sum certain for injury to or loss of property, personal injury, or death; and the signature of the claimant or claimant's authorized representative. The claims examiner also compares the written claim with the claims record in CMS to ensure all the information was uploaded correctly. Once a claim is deemed legally sufficient and accurate in CMS, the claims examiner investigates the claim by collecting evidence and interviewing personnel. For example, the claims examiner may request that airport security personnel review airport CCTV footage or the examiner may interview airport staff and other witnesses to the incident. At the completion of the investigation, the claims examiner recommends to the Delegated Authority Official (DAO) approval, settlement, or denial of the claim. Finally, the DAO adjudicates the claim.

Upon adjudication, TSA sends the claimant a determination letter. If TSA determines payment is warranted, the determination letter includes a payment form that collects the claimant's Social Security number (SSN) or other taxpayer identifier and bank account information in order

to remit payment via an Electronic Funds Transfer (ETF).[8] If it is determined that no payment will be made, TSA sends a denial letter with instructions for follow-up and how to contact TSA for any questions about the denial. If the claimant is dissatisfied with TSA's decision on an FTCA claim, he or she may file suit in the appropriate U.S. District Court not later than six months after the date of mailing of the notification. If the claimant has new or additional information that was not submitted with the initial claim, the claimant may request reconsideration. TSA's decision on MPCECA claims is final and unreviewable, but an employee may ask for reconsideration if there are facts or circumstances not raised or properly considered in the original claim.

TSA may share information collected as part of the claims process with third parties in accordance with the Privacy Act of 1974 and DHS/ALL-013 Department of Homeland Security Claims System of Records Notice (SORN).[9] Any information concerning violations or potential violations of law or regulation, including fraudulent claims, may be shared within the Department of Homeland Security (DHS) and with the appropriate federal, state, or local law enforcement agencies. TSA may share claimant information with the U.S. Department of Justice (DOJ) for the purposes of helping TSA prosecute criminal violators, or representing TSA in litigation or for approving certain claims. For approved claims, TSA will share with U.S. Coast Guard's Finance Center (USCG FINCEN) (payments up to $2,500) and with the Department of Treasury (Treasury) (payments over $2,500) the claimant's name, address, SSN, and banking information for payment.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Under the FTCA at 28 U.S.C. §§ 1346(b), 1402(b), 2401(b), 2671-2680, with implementing regulations at 28 C.F.R. Parts 14.1-14.11, a legally sufficient claim must include the claimant's signature or the signature of claimant's authorized representative, a demand for money damages in a sum certain, and a description of the incident sufficient to permit TSA to investigate fully. Under MPCECA, found at 31 U.S.C. § 3721, the claimant must submit a claim in writing within two years after the employee discovers or should have discovered the loss or damage. The claim must be signed by the employee. When payment is found to be warranted, the collection of a taxpayer's identifying number and bank account information is required by Treasury for all government payments to the public pursuant to 31 U.S.C. §§ 3325(d), 3332. DHS Management Directive (MD) No. 1650.1, *Personal Property Claims and Tort Claims*, and TSA MD No. 1000.15, *Claims Management* also provides agency policy and procedures for claims processing at TSA.

[8] Claimants may receive payment by check upon request.
[9] DHS/ALL-013 Department of Homeland Security Claims Records, 73 FR 63987 (October 28, 2008).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

- DHS/ALL-013 Department of Homeland Security Claims Records, 73 FR 57642 (October 28, 2008).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, a three-year security authorization was granted for CMS on October 1, 2016.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, the CMS records retention schedule of seven years is approved by NARA (General Records Schedule (GRS) 1.1, Item 80).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The OMB control number is 1652-0039.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The following information is collected on the SF 95:

- Claimant's contact information, including full name; signature; mailing address; phone number; and email address. Claimant's type of employment (military or civilian); date of birth (DOB); marital status; and if claimant was on official travel or not. If the claimant is under 18, a parent or legal guardian may file on his or her behalf. Documentation proving parental relationship or legal guardianship must be provided by individuals representing underage claimants; e.g., a birth certificate or other legal document.
- The claimant representative's name and contact information, if applicable. (If not collected on the SF 95, the claimant must provide to TSA via mail, email, or fax, written authorization that TSA may share information with the representative.) The name and contact information of the property owner, if not the claimant, also is collected.

- Date and time of incident and the basis for the claim including the known facts and circumstances attending the damage, injury or death; any other persons involved; a description of the property involved; the nature and extent of damage and location where property can be inspected; the place of occurrence and the cause thereof; the names and contact information for up to three witnesses; the monetary amount claimed; if any report or claim was filed with the airline, airport, or law enforcement agency; and any insurance coverage including the policy number.
- TSA's SF 95 supplemental form collects travel information such as air carrier, flight numbers, airport location, baggage tag numbers (if any).

The following information is collected on the DD 1842 and DD 1844:

- Claimant's contact information, including full name; branch of service and rank (when applicable); SSN; signature; mailing address and/or military duty address; phone number; and duty phone number (when applicable claimant's type of employment (military or civilian); and amount claimed.
- Date and location of the incident and the basis for the claim including the known facts and circumstances attending the damage; a description of the property involved; and the nature and extent of damage.
- Name of private insurance; policy number; claim numbers; inventory date; original cost; claims made against a private insurer; name of carrier or warehouse firm that has paid or repaired the claimed property; any claimed property owned by the Government or someone other than a family member; and any other claimed items acquired or held for sale, or acquired or used in a private profession (all of the aforementioned where applicable).

While not required, TSA recommends providing, when possible, purchase receipt of the original item lost or damaged (or credit card, banking statements, or other item appraisal); copies of boarding passes and baggage tags, or any other air carrier or TSA documents related to the travel; repair estimates; replacement estimates; photographs of lost/damaged items (past or present); police, witness or other incident reports (if applicable); and any air carrier or other claim reports.

2.2 What are the sources of the information and how is the information collected for the project?

Information is collected directly from the claimant or his or her authorized representative. Claims must be submitted to TSA in writing within two years of the incident. Claimants can mail, email, or fax completed and signed claims packages (SF 95 and SF 95 *Supplemental Information* or DD 1842 and DD 1844, or other form to be determined of necessary.) to:

TSA Claims Management Office
Claims, Outreach, and Debt Branch
701 South 12th Street, TSA-9
Arlington, VA 20598-6009
Fax: (571) 227-1901
Email: tsaclaimsoffice@tsa.dhs.gov

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, CMS does not collect or use information from commercial sources or publicly available data to adjudicate claims.

2.4 Discuss how accuracy of the data is ensured.

While the information is provided directly by the claimant, or his or her representative, and therefore presumed to be accurate, each claim is reviewed for legal sufficiency and accuracy before beginning an investigation. During this review, the claims examiner checks for claimant signature; ensures the claim was filed within two years of the incident date; the specific date of the loss or property damage; the location of the incident; the circumstances of the loss or damage property; and the sum certain claimed. The examiner also verifies that the written claim information was uploaded correctly into CMS. During the investigation, the examiner will gather all supporting documentation in order to make a recommendation to the DAO. When the DAO reviews the recommendation, the DAO also makes sure that the documentation supports the claim examiner's recommendation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that incorrect PII will be collected as part of the claims submission process.

Mitigation: This risk is mitigated. Each claim is verified through the adjudication process and by communicating with the claimant. Tort claims are filed directly by the individual or his or

her representative and are therefore assumed to be accurate. The SF 95 was developed to collect the minimum amount of information needed to process a claim and to reduce opportunities for submitting inaccurate, or unnecessary information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA uses the information collected to investigate and adjudicate claims against the agency.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, CMS does not perform electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly; however, in some cases, the information may be used to identify victims of theft or to further criminal investigations into property theft. For example, TSA Investigations may use claims information to identify possible trends of theft.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, although no other DHS component has assigned roles or responsibilities within CMS, TSA's Investigations office may access this system to identify victims of theft or other criminal matters. Additionally, TSA Customer Service Managers at airports receive an automatically generated email when claims are entered into CMS to alert them when an investigation is needed at his or her airport. Furthermore, the United States Coast Guard's Finance Center receives the claimant's bank account information to share with Treasury when a claim is approved so that payment can be issued.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected may be used for purposes other than adjudication of claims.

Mitigation: This risk is mitigated because all claims records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. Information collected by CMS will be used only in accordance with the described uses in this PIA and its respective SORNs by integrating administrative, technical, and physical security controls that place limitations on the collection of PII, and protect PII against unauthorized disclosure, use, modification, or destruction. System users

receive privacy training, and system managers were involved in the drafting of this PIA. Any TSA personnel discovered to have used or accessed CMS data inappropriately may be subject to disciplinary actions and/or may lose access to CMS.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why.

The FTCA establishes an individual's rights with regard to filing a claim and governs the way claims are processed. General information about the FTCA is available on the DOJ's website.[10] Notice of how to file a claim against TSA may be found on TSA's website.[11] Additionally, DHS provides MPCECA policy and process direction for filing claims in DHS Management Directive 1650.1.[12]

Submission of a claim against TSA is voluntary and initiated by the individual so he or she is aware that TSA will collect and maintain the claimant's information.. If using a representative, TSA requires written authorization from the claimant before TSA will share information with the representative. This authorization helps to ensure that the individual is aware that a claim is being filed on his or her behalf and that TSA is collecting his or her information. There are also Privacy Act Statements on the SF 95 and SF 95 *Supplemental Information* forms and the DD 1842 that provide notice to the claimant of how his or her information may be shared external to the agency and the potential consequences of not providing all the requested information. Finally, the program's PIA and applicable SORNs provide further notice to individuals.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Submission of a claim is voluntary and initiated by the individual. A claimant can withdraw a claim at any time or can choose to provide only limited information; however, failure to develop a sufficient claim may prevent TSA from being able to fully investigate a claim or award payment.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a small risk that a claim may include personal information belonging to someone other than the claimant without his or her knowledge, such as the name and contact information of up to three witnesses, or when a claim for damages is submitted by the individual who traveled with the property and not the property owner.

[10] DOJ Tort litigation website: https://www.justice.gov/civil/federal-tort-claims-act-litigation-section.
[11] TSA claims website: https://www.tsa.gov/travel/passenger-support/claims.
[12] Policy and process directive for personal property claims and tort claims at DHS MD 1650.1.

Mitigation: This risk is partially mitigated. TSA advises claimants to obtain witnesses' and/or property owners' permission to include their contact information. The SF 95 includes a Privacy Act Statement that claimants may share with witnesses and property owners to provide them notice of the information collection and all authorized uses and sharing of CMS data. Furthermore, the authorized uses and sharing of claims information are published for the public's awareness in this PIA and in the applicable SORNs.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

Records of monetary or property claims against TSA are maintained for at least seven years after final action in accordance with NARA's General Records Schedule (GRS) 1.1, Item 80, in order to maintain a historical record of submitted claims and their resolution.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that TSA will retain more data than is necessary or will retain data for periods of time longer than approved.

Mitigation: This risk is mitigated as TSA makes every attempt to only collect information needed to adjudicate a claim while maintaining claims records for the minimum amount of time required – seven years. This retention period is necessary to ensure TSA has adequate time to review, investigate, and respond to claims, as well as maintain a historical record of recent claims and their resolution, and time enough to address any potential disputes or litigation that may arise after the claim is processed. TSA enforces the records schedule by reviewing all records older than seven years on an annual basis. Then the Claims Program Manager reviews each and deletes those that are no longer needed for a business use in accordance with NARA General Records Schedule 1.1, Item 80.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As part of normal agency operations, TSA shares claimant information with the DOJ if a case is to be litigated, and with Treasury for issuing payment, when warranted.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS/ALL-013 Routine Use A allows TSA to share claimant information with DOJ when a case is going to be litigated in court. This sharing is compatible with the original collection because DOJ will represent TSA in court in order to resolve the claim.

Routine Use F allows TSA to share claimant information with "contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to [the] system of records;" thus, sharing with Treasury for the purpose of issuing payment on awarded claims is allowable under Routine Use F. This sharing is compatible with the original collection because Treasury will facilitate payment of awarded claims to individuals.

6.3 Does the project place limitations on re-dissemination?

No, TSA does not place limits on re-dissemination of information. The most common sharing is with the Treasury Department and the U.S. Coast Guard for payments. When transmitting payment information to the Treasury, TSA uses a Judgement Fund Document Submission Cover Sheet that states, "Sensitive but Unclassified" to help protect the contents. Payment information for awarded claims under $2,500.00 are transmitted within DHS to the U.S. Coast Guard via an encrypted file. To the extent an individual is covered by the Privacy Act, TSA limits its disclosures to those permitted under the Privacy Act and recipient federal agencies would likewise be limited in re-disseminating information. Re-dissemination may occur, for example, if TSA provides claimant information to Treasury who concludes that it is appropriate to further disclose it to a State tax authority or other agency.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Claimants' banking information is shared with either USCG FINCEN (payments up to $2,500) or Treasury (payments over $2,500) to facilitate payment for all awarded claims. Awarded claims are annotated as having been disclosed to USCG FINCEN or Treasury in CMS. All other disclosures are tracked manually by the Claims Branch Manager and processed by TSA's Freedom of Information Act Branch.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that PII may be shared with persons without a need-to-know or recipients may not secure PII properly.

Mitigation: TSA properly marks all documents as to their sensitivity level, provides requirements for secure access along with the exchange of information, and uses appropriate transmittal mechanisms. Any risk in sharing of banking information for claims over $2,500 is mitigated with three Treasury forms before Treasury will begin to process the settlement. These three forms are Form 194: Judgment Fund Transmittal, Form 196: Judgment Fund Award Data Sheet, and Form 197: Judgment Fund Voucher for Payment, all of which are protected. Treasury is governed by instructions include proper handling and protections for PII such as disclosing only to individuals with a need-to-know in the performance of their duties in accordance with the Privacy Act of 1974. Additionally, payments for over $2,500 are made by the Treasury's Judgement Fund. TSA sends requests for payments under $2,500 within DHS to the USCG FINCEN with a Tort Claim Approval Letter.

Section 7.0 Redress

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

Individuals, regardless of immigration status, may seek access to their information by submitting a request to:

TSA Headquarters FOIA Office
FOIA Officer, Transportation Security Administration
701 South 12th Street, TSA-20
Arlington, VA 20598-6020
Fax: 571-227-1406
Email: FOIA.TSA@dhs.gov

Instructions on how to request records from TSA may also be found here: https://www.tsa.gov/foia/requests.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals covered by the Privacy Act may seek to amend or correct records by submitting a request pursuant to the Privacy Act. Instructions may be found at www.TSA.gov under the FOIA link in Section 7.1. In addition, all individuals may amend their claim record at any time prior to final agency action or prior to the exercise of the claimant's option to file suit in U.S. District Court.

7.3 How does the project notify individuals about the procedures for correcting their information?

TSA provides information on submitting requests under the Privacy Act and Freedom of Information Act on its public website at www.TSA.gov. TSA provides information on the reconsideration process in the denial letter mailed to claimants.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that claimants cannot appeal the decision within TSA.

Mitigation: This risk is mitigated. Claimants may file suit in U.S. District Court if the claim has been denied or not resolved within six months.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The CMS Information Technology (IT) System Security Plan (SSP) describes the auditing measures and technical safeguards in place to prevent misuse of claims data. Data integrity, privacy, and security were a vital part of the system design in the following ways. For example, a server intrusion detection system and network intrusion detection system automatically and constantly monitor all login traffic. The system also automatically undergoes penetration testing, to monitor any attempt to hack into the system. Under this SSP, CMS is audited annually for IT security policy compliance and technical vulnerabilities by the TSA IT Security Office.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS provides privacy training in an online course on an annual basis to all DHS personnel.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The CMS is a role-based system in which the TSA Program Manager grants access to authorized users based on their position and duties. Only personnel with a valid need-to-know for the performance of their duties are granted access to CMS.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any new MOUs or data sharing agreements are reviewed by the TSA Claims Branch Chief, the Financial Management Director, Chief Financial Officer and the TSA Chief Counsel's office, with input from the TSA Privacy Officer and/or TSA Chief Information Security Officer, as needed, before submitted to DHS for final approval.

Responsible Officials

Sherry Johnson, Claims Branch Manager
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security