Transportation Management Services System (TMSS) 2.0

Privacy Impact Assessment

March 26, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. It requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses processes; and can cover all of the systems, applications or projects logically necessary to conduct that business.

The document is designed to guide GSA program managers, system owners, system managers and developers as they assess potential privacy risks during the early stages of development and throughout the system, application or project's life cycle.

The completed PIA shows how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:
https://www.gsa.gov/portal/getMediaData?mediaId=167954

Please send any completed PIAs or questions to gsa.privacyact@gsa.gov.

Stakeholders

Name of Information System Security Manager (ISSM)

- Joseph Hoyt

Name of Program Manager/System Owner

- Narendra Rao Namana Mohanakrishna

Signature Page

Signed:

DocuSigned by:

Joseph Hoyt

CA8EF810EDA7425...

Information System Security Manager (ISSM)

DocuSigned by:

Narendra Rao Namana Mohanakrishna

776FE828D4EF405...

Program Manager/System Owner

DocuSigned by:

Richard Speidel

171D5411183F40A...

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for making sure the PIA contains complete privacy related information.

Document Revision History

Date	Description	Version of Template
11/26/2019	Initial Draft of PIA Update	1.0
12/16/2019	Updated and Reviewed Comments	2.0
3/26/2020	Final Draft	3.0

Table of contents

Document purpose

This document contains important details about how and why the *TMSS 2.0. GSA Travel and Transportation Office* may, in the course of *Move Management*, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

System, Application or Project

TMSS - Transportation Management Services Solution

System, application or project includes information about

TMSS is an online freight and household goods transportation management system designed exclusively for federal civilian agencies, providing access to GSA's highly competitive transportation rates via the Freight Management Program (FMP) & Centralized Household Goods Traffic Management Program (CHAMP). This application is used across agencies.

System, application or project includes

User's name, address, email and phone number. Shipping addresses or household goods shipments (home addresses). Business information (business name, business address, tax identification number (TIN), etc.): Transportation service provider (TSP) business names, addresses, email addresses, phone, POCs, etc. Platform-related information (IP address, cookies, form data, third party services, for ex., code.jquery.com and google-analytics.com, etc.: User IP addresses (audit logs), session and authentication tokens/cookies, and federated analytics tracking code.

Overview

Transportation Management Services Solutions (TMSS) 2.0 is a GSA cloud-based, agile rate procurement solution that supports federal agency transportation requirements for the worldwide shipment of household goods and freight. TMSS 2.0 offers federal agency customers access to the Centralized Household Goods Traffic Management Program (CHAMP) and the Freight Management Program (FMP) which both provide comprehensive tenders of service, vetted suppliers, highly competitive rates, consistent pricing structure, and a customer satisfaction index built into the program.

Information about the individual who is moving (Name, To / From Address, Phone Number) is collected from end user data entry. This information is provided to the various Transportation Service Providers who are contracted with GSA to provide moving services for purposes of providing availability and pricing for comparison to offer best value / pricing to the Government for the employee’s move. These TSPs are registered users of the system.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA must collect the contact information about the Requester / User as well as the from / to moving addresses so that TSPs can provide estimates for their move request and so GSA can provide this information back to the requester.

1.2 What legal authority and/or agreements allow GSA to collect the information?

The Federal Acquisition Regulation (FAR) , Subpart A-General; part 47,
“Transportation”.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

The PII in TMSS is not searchable by a unique identifier. Instead, transactions are searchable by transaction id. The ID is alphanumeric, where a sequentially generated number is concatenated to a single letter prefix (for example P001, P002, P003).

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

This is not applicable because the individuals providing information are government employees. Therefore, no information collection request has been submitted to OMB.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

The retention schedule for this System's records (such as shipment booking and rates) is 7 years. It is based on the requirement from the business line, since some of the rates data can be used for auditing, which has a 7 year data retention requirement.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

On the Household Goods side of the system collects employee name and move from / to address. The system requires SSO (Single Sign On) authentication for Gov Employees and Two Factor Authentication for Non-Gov Employee Users.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Yes, individuals are given notice prior to the collection of personal information

https://moveit.gsa.gov/: "This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution." However, no

Privacy Act statement is presented because PII in TMSS is not searchable by a unique identifier.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No, there are no significant privacy risks for this system that relate to openness and transparency.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

TMSS maintains information about GSA Employees, Non GSA Federal Civilian Agencies Personnel, and Transportation Service Providers.

3.2 What PII will the system, application or project include?

The information that is being collected are Contact information for shipment, Business information, individuals name, address for household goods shipment and platform-related information.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

The personal information such as Name and address are used for the preparation, shipment and confirmation that personal goods reached their intended destination intact.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No the system will not create any new data about individuals.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

FAS Cloud Services (FCS) is responsible for protecting and preventing unauthorized access to the application and data.

3.6 Will the system monitor the public, GSA employees or contractors?

No, the application does not have the capability to monitor the public, GSA employees or contractors. Even though the system provides transportation capabilities, the system does not monitor and track employee movement. Monitoring employee movement is not the intent of TMSS

3.7 What kinds of report(s) can be produced on individuals?

Shipment Reports, User Reports, Transaction Reports. These reports provide data related to shipments information like origin, destination, package details, date of shipping etc. Some of the reports include details about the Transportation Service Providers who are in the system. Other reports include details about the rates being filed for transportation. Reports are for listing TSPs, users of a given agency, shipment reports (reports files by TSPs to let the government know of the business they have done for a given period). The business line has access to the reports.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

No, reports are not de-identified. Reporting is not done on an individual level. The only report that lists an individual's name is the user agency report, telling who can access TMSS for a given agency and bureau.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

No, the system limits personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed. Only the absolutely required data elements for setting up a user record are collected (Name, office address, phone, email). Data is stored in a database (Amazon RDS) in FAS Cloud Services which has its own security perimeters and parameters. Amazon S3 (Simple Storage Service) is used for rate files uploaded by the TSPs (Telecommunications Service Provider). S3 buckets are assigned to each application and access to the folder structure within S3 is controlled by FCS security measures. FCS has an ATO for each service that it provides.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Yes, the contact information collection is used for Government employees who are physically moving themselves and their household goods. TMSS application does not have the capability of contacting employees via the application

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

Yes, information will be shared with Transportation Service Providers and Non-GSA Federal Civilian agencies. The civilian agencies only can access data about their employees within the agency. The information is shared by way of reports run within the system.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Yes, Information is collected directly from the individual and/or Agency Move Coordinator.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

Yes the system interacts via API with Syncada, PCMiler (is a Web service provided by Trimble maps to retrieve distance/mileage between 2 addresses). There are formal agreements with the business line.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

There are no privacy risks with external information sharing.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

The end user is responsible for data accuracy and completeness. The system processes zip code, state code, country code for validation. The agency move coordinator role doesn’t apply.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

Currently, risk associated with individual information has not been identified.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

TMSS is a single Database application. Only GSA employees and contractors Database and System Administrators will have access to the data within the database. Application users who run reports will have access to export data.

TMSS is a role-based application. All user registration is monitored and access is granted only by system administrators after verification.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, an SSP has been submitted to the security office and the assessment has been completed and is currently undergoing an internal QA process.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

The system in housed in Secure, FAS Cloud. The system incorporates single sign on and two-factor authentication. The User Management applies strict role based access controls around what end users are authorized to do within the system.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

FCS Cloud team is responsible to implement mechanisms to identify security breaches. The mechanism is in accordance with GSA security incidents and breaches for PII policy and procedure. TMSS application and data owners will be notified by platform and NETOps personnel of any breaches. IDS and SEIM tools are part of the cloud.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

TMSS application only gathers and captures the absolutely required data for application users. Tax identification numbers of any type are not captured by the TMSS application.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

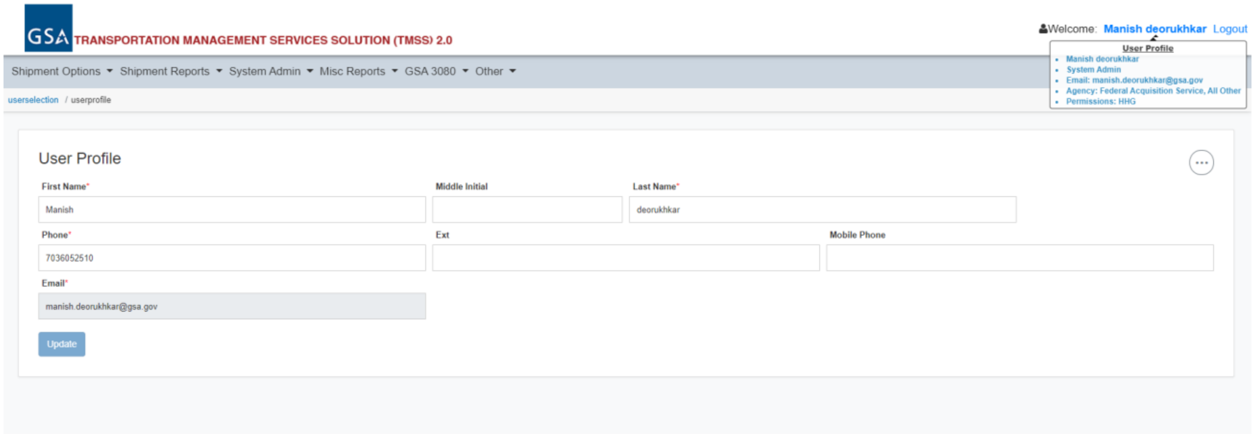
Individuals have the option for providing information. However, if goods must be shipped from origin to destination, then accurate information must be provided.

7.2 What procedures allow individuals to access their information?

Individuals can access their information through the TMSS Reporting Modules.

7.3 Can individuals amend information about themselves? If so, how?

Individuals can update information about themselves via the edit profile screen.


GSA
TRANSPORTATION MANAGEMENT SERVICES SOLUTION (TMSS) 2.0
Welcome: Manish deorukhkar Logout
Shipment Options
Shipment Reports
System Admin
Misc Reports
GSA 3080
Other
userselection / userprofile
Update

User Profile

- Manish deorukhkar
- System Admin
- Email: manish.deorukhkar@gsa.gov
- Agency: Federal Acquisition Service, All Other
- Permissions: HHG

User Profile

First Name*: Manish

Middle Initial:

Last Name*: deorukhkar

Phone*: 7036052510

Ext:

Mobile Phone:

Email*: manish.deorukhkar@gsa.gov

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

No privacy risks have been identified.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

GSA has developed, implemented, and regularly updates its IT Security Awareness and Privacy Training as part of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

Government employees and contractors are required to take annual privacy and security training. A Terms of Service pop up box with details around Policy & Regulation provided, must be accepted.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

No there are no privacy risk related to awareness and training. ISP provides annual security and awareness which includes privacy training. The FCS Security Incident Response Plan scope pertains to FCS team capability for detecting, reporting, and responding to security incidents.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

The application will generate logs for auditing. All CRUD (Create, Read, Update, Delete) are logged. The FCS logs are auto created and maintained in Splunk. Access control has been implemented to track access and prevent unauthorized access. PII information will be restricted to only authorized personnel. Also, Various transaction history audit trail such as ratefilig, rate query, Shipment creation, IFF filings, Survey filings, are stored to the TMSS database as and when the user creates, updates, assign, terminate, and delete the transactions.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

There are no privacy risks associated with accountability, access to application risks is restricted. Various transaction history audit trails are stored in the TMSS database.

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” The memorandum notes that “because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.”

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.