Transportation Management Services System 2.0 (TMSS 2.0)

Privacy Impact Assessment (PIA)

April 6, 2021

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. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business 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 builds privacy protections into technology from the start. Completed PIAs are available to the public at gsa.gov/pia.

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 that are codified in the Privacy Act of 1974.

Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response. Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **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 (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
3/18/2021	Minor edits (verbiage and format)	3.1
3/25/2021	Added GSA/GOVT-4 SORN Reference	3.2

Table of contents

SECTION 1.0 PURPOSE OF COLLECTION

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?

1.3 Has an 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.

1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice before to the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

SECTION 3.0 DATA MINIMIZATION

3.1 Why is the collection and use of the PII necessary to the project or system?

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

3.3 What controls exist to protect the consolidated data and prevent unauthorized access?

3.4 Will the system monitor members of the public, GSA employees, or contractors?

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

3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

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, maintenance, use, or dissemination?

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?

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)?

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

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

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

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

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

SECTION 8.0 AWARENESS AND TRAINING

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

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about Transportation Management Services System 2.0 (TMSS 2.0). To accomplish its mission, the Travel and Transportation Office must, 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, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

Transportation Management Services System 2.0 (TMSS 2.0)

B. 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.

C. For the categories listed above, how many records are there for each?

103,446 Contractor Records, 207,480 records for Federal customers (Shipment data - origin/pickup and destination/delivery addresses).

D. System, application, or project includes these data elements:

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 2.0 (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 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

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

1.2 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?

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). SORN ID: GSA/GOVT-4 for “Contracted Travel Services Program” applies to this PIA.

Please refer to the link below.

https://www.federalregister.gov/documents/2009/06/03/E9-12951/privacy-act-of-1974-notice-of-updated-systems-of-records

1.3 Has an 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.

1.4 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

SECTION 2.0 OPENNESS AND TRANSPARENCY

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

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes, individuals are given notice prior to the collection of personal information https://tmss.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.

SECTION 3.0 DATA MINIMIZATION

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

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.

3.2 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.

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

TMSS inherits the protections granted to it by the FCS FISMA system. On an application level, TMSS is an API driven application that utilizes TLS 1.2 with strong ciphers to protect all data in transit. Due to the non-sensitive nature of the information within TMSS, the S3 and the RDS Database are unencrypted outside of protections inherited by the FCS FISMA system.

3.4 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.

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

Shipment Reports, User Reports, Bill of Lading (BOL) Reports, and 3080s (GSA Form Name - Customer Satisfaction Survey). 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.

3.6 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.

SECTION 4.0 LIMITS ON USING AND SHARING 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 and how? 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), Okta, and

SecureAuth. There are formal agreements with the business line for Syncada and PCMiler, while Okta and SecureAuth are GSA syndicated SaaS products.

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, maintained, used, or disseminated 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.

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 (SSP) for the information system(s) or application?

Yes, an SSP has been submitted to the security office and the assessment has been completed with an ATO granted on 04/13/2020.

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

The system is located in AWS under FCS safe guards. It utilizes best practice MFA and SSO for user authentication with strict role based access controls around what they are authorized to do within the system. As an API driven application, all information in transit is encrypted using TLS 1.2 and strong ciphers as designated by NIST standards. The system does not house PII or PCI and all data within the system is non-sensitive in nature. There is no encryption of data at rest outside what is inherited from FCS. Administrative controls include regular yearly self-assessments, annual user recertifications, and daily database back ups with the ability to rapidly fail and rebuild.

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

The FCS team is responsible for implementation of mechanisms to identify security breaches. 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.

In addition to these safeguards, the application forwards all logs to Splunk for further auditing capability and the potential for automated alerts and reports while maintaining and application specific incident response plan tested annually.

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 do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Individuals have the option of not providing information as the usage of TMSS is strictly voluntary. 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.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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

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 owner ensure that the information is used only according to 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 rate filing, 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.

---

[1]OMB Memorandum *Preparing for and Responding to the 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.