Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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]

[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.

General Information

PIA Identifier: 398
System Name: Order Management System (OMS)
CPO Approval Date: 8/4/2022
PIA Expiration Date: 8/3/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Haven Wynne

Chief Privacy Officer (CPO) Approval

Laura Gerhardt

PIA Overview

A: System, Application, or Project Name:
Order Management System (OMS)

B: System, application, or project includes information about:
Includes information about sales orders, purchase orders, customer contact information, vendor information, in support of the GSA mission.

C: For the categories listed above, how many records are there for each?
There are multiple thousands of vendors, multiple millions of sales and purchase orders, and over a million customer contacts.

D: System, application, or project includes these data elements:
We have name and contact information, including home addresses as part of the GSA Advantage feed. We do not have SSN or similar information. We have financial information in tokenized format.

Overview:

- Descriptions of its purpose(s) – why this system, application, technology, pilot, program, or other collection (project) is being completed; what legislation authorizes it; and how it relates to the GSA's mission of providing the best value for government and the American people;

The GSA has acquired an Order Management Services (OMS) solution from IBM to achieve a more agile, flexible, and efficient supply chain. This will allow the General Supplies and Services (GSS) Office to adapt to rapidly-evolving customer requirements including greater reliance on direct vendor shipment of goods to customers. The GSS intends to be the preferred supply chain provider of the U.S. Federal Government and to support the associated business model transformation. The GSA OMS will achieve these capabilities and objectives through the SaaS delivery model.

The GSA OMS solution is housed in IBM's Smartcloud for Government (SCG). SCG is specifically designed to help government organizations respond to technology requirements more quickly. This Federal Information Security Management Act (FISMA)-compliant cloud environment is part of IBM's established and dedicated Federal Data Centers (FDC).
The FDC houses the GSA OMS solution elements, which include the following five primary SaaS components:
● IBM Sterling Order Management: Provides multi-channel order aggregation with global visibility to order status, shipment and limited financial information enabling the complete order to cash flow. With optimized, rules-based order promising and scheduling, requisitions are appropriately allocated to meet the conditions of the order and the requirements of GSA business. Throughout the lifecycle of the requisition, status information and related data is recorded in OMS from various sources. End users with appropriate authorization can manage requisitions and lookup requisition status information, purchase orders and purchase order status information, customer information, and catalog information.
● IBM Integration Bus: Provides a fast, simple way for systems and application to communicate with each other. It offers a robust capability to address diverse integration requirements with external GSA systems. Delivers a standardized, simplified and flexible integration foundation to help GSA to quickly and easily support business needs and scale with business growth.
● IBM Sterling Business-to-Business (B2B) Integrator: Provides secure connectivity and collaboration with customers, suppliers/vendors, and business partners. It provides the capabilities necessary to automate B2B processes, managed file transfers, and direct application integrations. With its capabilities to provide dynamic workflow management, file translations on the fly, and a robust any-to-any internet protocol gateway capability, the B2B Integrator is leveraged to integrate external partner processes with the overall IBM OMS solution as well as other GSA solutions and systems.
● IBM Analytics (Cognos): Provides the capability to identify trends, online/offline order patterns, and supplier reports. These analytics are accessible in a variety of required formats to assist GSS leadership in analyzing data and making critical business decisions related to the optimization of the business. It provides the capability to generate pre-defined or ad-hoc reports, scorecards, dashboards, as well as conduct data analysis and real time monitoring.
● IBM WebSphere Portal (Vendor Portal): Provides the capability to aggregate content from multiple services from within and external to the SaaS solution in a portal interaction environment. To achieve the key capability of providing visibility to the vendor end-user, the IBM OMS solution leverages the WebSphere portal to view purchaser order information, to acknowledge receipt of the purchase order, and to record ASN (Advance Shipment Notice) information.

The OMS architecture should be considered as an integration of these five COTS packages, with local customization which uses an application extensibility framework and additional integration tooling (e.g. SAML components on a WebSphere platform, integration with GSA systems etc.)

- Descriptions of what PII is collected, its maintenance, use, or its dissemination and who or what it is collected from; and,

Based upon the GSA Advantage PIA, OMS will be receiving PII information from that source.

- Descriptions of how the system, application, or project collects and uses PII, including an example that illustrates what happens to the PII from the time it is collected until it is destroyed.

We receive a feed from GSA Advantage over an ssh protected tunnel. The data is parsed, and the PII in the form of a shipping address is stored as part of the order fulfillment process. That information is then fed to upstream systems, including but not limited to vendor systems, PO Data interfaces, ECMS, and Vision.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
OMS does not collect or maintain PII. It uses and disseminates the information under the agreements maintained by GSA Advantage.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
No

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
This information is part of the retention of all financial transaction information (seven years).

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.
OMS does not provide notice to the individuals; that task is performed by GSA Advantage, who collects and uses that information.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
OMS does not control the information collected by GSA Advantage, but ingests it from the feed. It is necessary to complete the fulfilment of a shipping order.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
Additional controls have not yet been implemented, and are awaiting a contract approval. Expected controls include encryption of data at rest and in transit.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
OMS does not have a specific monitoring capability.

3.5 What kinds of report(s) can be produced on individuals?
OMS has the ability to determine order information for an AAC (the equivalent of an office facility) and generate reports thereby. It is possible to then display orders within that AAC and identify individuals in that fashion.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
The requirement for de-identification has not been determined.

4.0 Limits on Using and Sharing 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?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Other Individuals

4.2How: If so, how will GSA share the information?
Shipping addresses are part of the required information for a purchase order. Fulfilment occurs via a variety of means, including the groups above with feeds to various agencies.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
OMS receives the feed from GSA Advantage.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?
Yes, OMS has multiple connecting systems, as described in the SSPP.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
OMS will not verify for accuracy or completeness. OMS utilizes the ship-to address based upon what is provided.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Access includes authorized GSA users, authorized GSA contractors, authorized GSA Vendors/Suppliers.

6.1b: What is the authorization process to gain access?
Authorization is controlled by the GSA Business Unit, through a formal workflow implemented in ServiceNow.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
7/14/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
OMS is operated in a FedRAMP facility with oversight via the controls specified in the GSA approved SSPP.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
There are a variety of controls, including intrusion detection monitored by the CSP SIEM; host integrity controls; anomaly detection; hardened software environment, and continuous monitoring through weekly and monthly analysis with quarterly reporting.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
OMS does not interact with individuals with regard to the shipping address. GSA Advantage, as the collector of the information, would monitor the consent/decline function.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?
OMS does not provide individual access; this would occur through GSA Advantage.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
OMS does not provide privacy training to end users. As contractors, we do undergo the GSA provided privacy training.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
The shipping address is only used for order fulfilment.