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: 414
System Name: VISION
CPO Approval Date: 4/4/2023
PIA Expiration Date: 4/3/2026

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
VISION

B: System, application, or project includes information about:
The Vision application is the primary user interface for the National Customer Service Center (NCSC) customer service agents to handle customer agency, vendor, and private citizen calls, emails, live chats.

C: For the categories listed above, how many records are there for each?
Estimated total of Customer Contact - 869,000, Private Citizen contact information 47,230, Vendors - 193,883 contact information which includes First Name, Last Name, business address, business emails, and business phone numbers.

D: System, application, or project includes these data elements:
Government Contact:

- First Name, Last Name, Street, City, State, Zip Code, Country, Agency, Bureau, Business Phone, Mobile Phone, Email, Service, Rank, Activity Address

Vendor Contact:

- First Name, Last Name, Street, City State, Zip, Country, Primary Phone, Mobile Phone, email

Private Citizen:

- First Name, Last Name, Street Address, City, State, Zip code, Country, Phone, Mobile phone, email

Overview:

The Salesforce Vision application is a subset of Salesforce Customer Relationship Management (CRM) application. The VISION system is built upon the Salesforce Service Cloud Platform as a Service (PaaS) implementation. The general purpose of the system is the primary user interface for the National Customer Service Center (NCSC), customer service agents to handle agency and vendor customer calls, enter case information, update resolutions, provide knowledge article information, and track incoming inquires.
AskGSA is a self-service Salesforce Community for GSA Global Supply Customers. The application has 2 primary roles. First, to allows customers perform order search functionality on GSA Global Supply orders with connections to GSA Global Supply Order Management System. Second, allows uses the ability to report problems on those orders through NCSC case management.
The VISION system involves connections to backend internal GSA systems via the FAS Enterprise Software Oriented Architecture infrastructure, and connections to the legacy VISS database. There is also a connection to the NSCS using NICE IN Contact telephony solution that has been granted an ATO from the OCISO's office pursuant to integration within Salesforce. This will provide the ability to log in to the Salesforce Vision Service Console softphone and receive inbound calls and navigate to telephone number fields and place outbound calls.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The FAS Salesforce Minor App – VISION currently has a SORN "GSA/CEO-1" which details the legal authorities to collect the information: 5 U.S.C. 301; 40 U.S.C. 11315; 44 U.S.C. 3506; E.O. 9397, as amended; E-Government Act of 2002 (Pub. L. 107- 347); Pub. L. 106-58 (Title VI, Section 643).

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
Currently listed in the Federal Registar - "GSA/CEO-1"

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.
The case management records fall within the following General Records Schedules and a blanket max retention of 6 years is applied to all case management records.
GRS 5.8 Administrative Help Desk Records
GRS 6.5 Public Customer Service Records
GRS 1.1 Financial Management and Reporting Records

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? Yes

2.1 Explain: If not, please explain.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The collection of PII data is necessary to support inquiries related to GSA programs and resolve those inquiries.

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?
This control is implemented by the Salesforce Customer Engagement Organization (CEO Org). Assigned authorizations for controlling access are enforced through Force.com Administration Setup Permission Sets & Public Groups.

1.) Practice least privilege permissions, where any user of the Vision Salesforce app will have only the minimum privileges necessary to perform their particular job function.

2.) Assign a designated application owner. That application owner will receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application); attend Security briefings, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team; work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

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

3.4 Explain: Please elaborate as needed.
No, the system does not monitor the public, employees or contractors. All logs of internal GSA associates who access the system are reviewed on a monthly basis per GSA policy.

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

The reports that can be produced on individuals are contact management, account management, and case management reports.

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 Vision application data is not share outside of GSA Federal Acquisition Services.

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?
None

4.2How: If so, how will GSA share the information?
N/A

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

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?

- Data leaving GSA and shared with an external agency
- GSA: via Pegasys Connect: All the financial adjustments to the customer are sent to the Pegasys Connect application. The following information is passed to FedPay: Requisition, financial adjustment, POC.
- DLA: via WebSDR Response: Requisition, Resolution codes and comments from Vision
- Fed pay: All the financial adjustments to the Vendors are sent to Fed pay. The following is the information sent to Fed pay: Requisition, financial adjustment, POC.

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?
The Program Manager and Application Owner are responsible for ensuring data is monitored for relevance and accuracy. In addition, the information is being directly provided by the individuals or indirectly provided by parties

acting on behalf of the individual and whom the individual had contacted. It is the responsibility of the individual to assure the data provided is correct.
As inquiries come into the NCSC the relevant contact information is updated for accuracy.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Internal users within GSA Federal Acquisition Service with the required roles, profiles, and permission.

6.1b: What is the authorization process to gain access?
1. NCSC employee will need gsa.gov email account

2. 6-8 week training session prior to approval and access to Vision

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.
3/24/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
As Salesforce is a cloud-based product, the minor application is protected by a multitiered security process. The cloud platform along with GSA's implementation of security controls provides a robust security profile. The data is protected by multiple access controls to the data, including login controls, profiles within the application and permission sets in the program. Program management has authority to grant access to the application at all application levels. All higher level system support staff are granted access based upon need to know/requirement based needs.

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?
Intrusion systems at the agency level provide a layer of security monitoring. Access to the GSA ORG unit is reviewed on a weekly basis, application permission sets are annually reviewed by the application owner.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
NCSC customers are provided a Privacy Act Notice at the point the information is collected. They initiate the contact through the ASKGSA portal.
Individuals that call into the NCSC are not required to provide contact information for support.

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?
On the Ask GSA webpage, there is a privacy link and Privacy Act Notice. This privacy link

(https://www.gsa.gov/portal/content/116609) contains the privacy and security notice that includes a section on the information that GSA gathers, cookies, and what happens to the information that is sent to GSA. The Privacy Act Notice provides the legal authority to collect the information, the primary uses of the information and the effect of not providing it.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
On the Ask GSA webpage, there is a privacy link and Privacy Act Notice. This privacy link (https://www.gsa.gov/portal/content/116609) contains the privacy and security notice that includes a section on the information that GSA gathers, cookies, and what happens to the information that is sent to GSA. The Privacy Act Notice provides the legal authority to collect the information, the primary uses of the information and the effect of not providing it.

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.
All GSA employees and contractors with access to this system are required to complete IT Security Awareness and Privacy Training on an annual basis. Users who fail to comply may have all access to GSA systems revoked. High level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply will have access revoked.

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 system owner ensures information is shared to GSA, Federal Acquisition Service employees through users Profiles, Roles, and Permissions.