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: 356
System Name: Accounts Receivable Claim System (ARCS)
CPO Approval Date: 12/22/2021
PIA Expiration Date: 12/21/2024

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Jennifer Hanna

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Accounts Receivable Claim System (ARCS)

B: System, application, or project includes information about:
ARCS contains records of employees (payroll), vendors, business and members of the public (past employees for example).

C: For the categories listed above, how many records are there for each?
ARCS contains records related to approximately 55,000 employees/ individual debtors: and approximately 14,000 records related to businesses.

D: System, application, or project includes these data elements:
ARCS contains full names, full addresses, phone number and SSN - tax id numbers - not required for all.

ARCS uses SSN (Tax ID) for historical reporting and reference to track debtors. SSN numbers are masked as Tax Identification Numbers. ARCS contains Tax Identification Numbers.

Overview:

Accounts Receivable Claim System (ARCS) is a historical read-only version of the old ARCS application. There is no end user interaction in the application other than viewing historical data and demand letters. ARCS no longer sends or receives any new data, i.e., PII or otherwise, but it continues to retain all of the previously stored sensitive information and remains active today only for research purposes of historical data within the application. ACA Sorn was completed. ARCS is covered by ACA as a minor application

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The following laws, regulations, and policies were used to determine the security requirements for the GSA certification:

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information. Authorities for recording Social Security Numbers are E.O. 9397, 26 CFR 31.6011(b)–2, and 26 CFR 31.6109–1.

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?
Yes, you can search the ARCS application by individual debtor name.

ACA has a SORN that is under Pegasys, and ARCS is covered because it is a subsystem of ACA

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.
N/A ARCS complies with all GSA retention and disposal procedures specified by 1820.1 CIO P GSA Records Maintenance and Disposition System. Records contained in the ARCS system will be retained consistent with

section 2.2 of NARA General Records Schedule, “Employee Management Records”. See https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf

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.
No, the ARCS application contains read only PII data that has been in an archived status since 2017. No updates to the PII data has occurred since 2017.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
ARCS required PII (SSNs masked as Tax ID numbers) in order to verify the correct debtor was being tracked to monitor the Non-Federal debt portfolio for GSA. SSNs are required because they are unique to each individual.

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?
Protections are made via role authorization into the application with Secure Auth, encryption at rest - TDE, column level encryption

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

3.4 Explain: Please elaborate as needed.
No, the ARCS application is now read-only and used only for historical research. It no longer sends or receives any new data, PII or otherwise. ARCS will remain only as a historical repository/reporting system.

3.5 What kinds of report(s) can be produced on individuals?
None. No reports can be produced on individuals. The following correspondence letters are produced: final demand letter, claim letter, payroll claim letter, second demand letter, waste scrap demand letter.

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?
None. No reports can be produced on individuals. The following correspondence letters are produced: final demand letter, claim letter, payroll claim letter, second demand letter, waste scrap demand letter**.**

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?
No

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 the application does not collect any new information as the application is read only historical data and previously collected data from other sources.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
N/A. ARCS does not interact with other systems or applications or projects either within or external to the organization. This is a read-only, historical data application and previously collected data from other sources.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
N/A. ARCS does not interact with other systems or applications or projects either within or external to the organization. This is a read-only, historical data application and previously collected data from other sources.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
This is a read-only with historical data. Data was verified by the data owner when entered into the application before becoming a historical read-only application. The application data will be migrated on premises from the cfocap database. The application's data will be encrypted at rest and in transit.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Business lines that utilize the system, will request access via EARS/CAAM. Authorized users of ARCS and their specified access privileges can be identified and retrieved from the Enterprise Access Request System (EARS) and/or applicable database. The user is granted appropriate access to the system based on: (1) a valid access authorization; (2) intended system usage; and (3) other attributes as required by the organization or associated missions/business functions. The business line has access to both reports and data.

6.1b: What is the authorization process to gain access?
Access Requests - Appropriate approval for requests to establish accounts are required and in place via use of EARS where the access request process flow is as follows: User -> User Manager -> System Owner -> ISSO -> Implementer. EARS send automated email to appropriate individual(s) from beginning to end of such access request process. Termination of Accounts - Cancellation of user accounts who are separated or terminated or transferred or users who no longer have a need for access are manually initiated by user manager and/or ISSO via EARS that will result in the execute the account cancellation and dropping of the account.

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.
10/1/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The assets utilized for ARCS are within a federal data center and secured appropriately. Role-based access that is managed through EARS/CAAM/MFA process. Back-end access is implemented through multi-factor authentication. Perconna MySQL database is encrypted at rest with column level encryption. Data in transit is encrypted via TLS 1.2.

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?
ARCS leverages the GSA incident response guide. Any suspected incidents or security breaches of PII are to follow the necessary steps below:
Contact service desk - submit incident ticket. Ticket forward to GSA incident response team and privacy office if potential PII exposure was involved. The system owner and related system user and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer, along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency. All potential instances are to be reported and reported directly to the IC Service desk.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
N/A. ARCS application is a read-only historical application (meaning no new data has been received since 2017) and no longer collects PII or sensitive data. There is no debt collection process in the new ARCS application.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
N/A. ARCS application is a read-only historical application (meaning no new data has been received since 2017) and no longer collects PII or sensitive data. There is no debt collection process in the new ARCS application.

7.2: What are the procedures that allow individuals to access their information?
N/A. ARCS application is a read-only historical application (meaning no new data has been received since 2017) and no longer collects PII or sensitive data. There is no debt collection process in the new ARCS application.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
N/A. End-users do not have direct access to this data to be able to review/update 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 are required to take the annual IT Security and Awareness training. Also required to take the Reporting Incidents and Security Breach 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?

User accounts are annually reviewed (audited) and/or recertified based on their continued need for access as appropriate (role based access). This annual user recertification process is done automatically via EARS where EARS will send an automated email to the user manager based on the value in ‘Next Recertification Date’ column in EARS. The User’s manager at that time can either approve or deny or return a recertification request to the user based on the determination in evaluating the user's need for continued access. ARCS auditable events include (Audit-logs) with third party assessments and encryption.

1. Successful and unsuccessful logons
2. Successful and unsuccessful alter/insert/update/delete operations on the tables
3. Any change in objects, adding new objects, deleting objects
4. Create user, alter user and drop user
5. Privileged access (See paragraph above)