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: 373
System Name: GSA Credential and Identity Management System (GCIMS)
CPO Approval Date: 1/12/2023
PIA Expiration Date: 1/11/2026

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Erika Dinnie

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Credential and Identity Management System (GCIMS)

B: System, application, or project includes information about:
Individuals who require routine access to agency facilities and information technology systems, including:

a. Federal employees.

b. Contractors.

c. Child care workers and other temporary workers with similar access requirements.

The system does not maintain records on occasional visitors or short-term guests.

C: For the categories listed above, how many records are there for each?
There are approximately 26,558 federal employees and 299,192 contractor records (including child care workers) as of 2021.

D: System, application, or project includes these data elements:
Employee/contractor/other worker full name
● Social Security Number (SSN)
● Date of birth
● Place of birth
● Height
● Weight
● Hair color
● Eye color
● Sex
● Citizenship
● Non-US citizens only:
o Port of entry city and state
o Date of entry
o Less than 3-year US resident (yes or no)
● Occupation
● Summary report of investigation
● Investigation results and date
● File attachments containing PII (adjudication memos from OPM, Contractor Information Worksheets)
● Security Specialist Notes
● Investigation History Data
● Level of security clearance
● Date of issuance of security clearance
● Facial Image (recorded at enrollment station during MSO registration)
● Fingerprints (recorded at enrollment station during MSO registration)
● Organization/office of assignment
● Region
● Telephone number
● ID card issuance and expiration dates
● ID card number
● Emergency responder designation
● Home address and work location
● Emergency contact information
● Physical and logical access
● Contractors only:
o Contract company (also referred as vendor)
o Vendor Point of Contact (POC)
o Whether contract company is the prime or a subcontractor
o Name of prime if company is subcontractor
o Task order number, delivery order, or contract base number
o Contract start and end date
o Contract option years (yes or no)
o Names of previous companies on GSA contracts

Overview:

The GCIMS application is designed to track GSA employee and contractor status in the credentialing and background investigation processes. GSA management, users, and respective role holders will have the ability to record the initiation of a PIV card request for a particular applicant, as per the HSPD-12 and GSA specific requirements and

procedures, manage the person's organization/company and/or contract affiliation, as well as the overall credentialing and investigation status during the process progression. The application provides search capabilities for organization, contract, and person. A credential screen summarizes the employee/contractor's personal information, status, issued credential, and conducted investigation. GCIMS enables a user to track important dates in the credentialing process.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
GCIMS is authorized by 5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 40 U.S.C. 3101, 40 U.S.C. 11315, 44 U.S.C. 3602, E.O. 9397, as amended, and Homeland Security Presidential Directive 12 (HSPD-12).

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?
GCIMS SORN GSA/CIO-1, As described in GCIMS SORN GSA/CIO-1, the system allows for retrieval by a combination of first name, last name, and/or Social Security Number. Group records are retrieved by organizational code.

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.
The Supporting Statement for Information Collection Submission OMB Control Number 3090-0283.

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

- GRS 05.6/120 Personal Identification Credentials and Cards - Application and Activation Records Records about credential badges (such as smart cards) that are (1) based on the HSPD12 standards for identification cards issued to Federal employees, contractors, and affiliates, and (2) used to verify the identity of individuals seeking physical access to Federally controlled Government facilities, and logical access to Government information systems. Also referred to as Common Access Cards (CAC) cards, Personal Identity Verification (PIV) cards, and Homeland Security Presidential Directive 12 (HSPD-12) credentials.

Exclusion: Records of certain classes of Government employee identification cards, such as those covered under special-risk security provisions or 44 U.S.C. Section 3542, are covered by agency-specific schedules. Application and activation records. Applications and supporting documentation, such as chain-of-trust records, for identification credentials. Includes:

- application for identification card
- a log of activities that documents who took the action, what action was taken, when and where the action took place, and what data was collected
- lost or stolen credential documentation or police report

Note: GRS 3.2, Information Systems Security Records, covers applications for access to information systems. Note: Agencies must offer any records created prior to January 1, 1939, to the National Archives and Records Administration (NARA) before applying this disposition authority. Retention: Temporary. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2017-0006-0016 (GRS 05.6/120) GRS 03.2/031 System Access Records. Systems Requiring Special Accountability for Access These are user identification records associated with systems which are highly sensitive and potentially vulnerable. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:

- user profiles
- log-in files
- password files
- audit trail files and extracts
- system usage files
- cost-back files used to assess charges for system use

Exclusion 1. Excludes records relating to electronic signatures. Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement. Retention: Temporary. Destroy 6 years after the password is altered or user account is terminated, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2013-0006-0004 (GRS 03.2/031) GRS 04.2/130 Personally Identifiable Information Extracts System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify." Retention: Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate. Legal Authority: DAA-GRS-2013-0007-0012 (GRS 04.2/130) GRS 04.2/140 Personally Identifiable Information Extract Logs Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date. Retention: Temporary. Destroy when business use ceases. Legal Authority: DAA-GRS-2013-0007-0013 (GRS 04.2/140) GRS 04.2/191 CUI Information Sharing Agreements Agreements in which agencies agree to share CUI with non-executive branch entities (e.g., state and local police) and foreign entities that agree to protect the CUI . Exclusion: Contracts involving CUI and contractor access to CUI ; GRS 01.1, item 010 covers contracts. Retention: Temporary. Destroy 7 years after canceled or superseded, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2019-0001-0006 (GRS 04.2/191) GRS 05.2/020 Intermediary Records Records of an intermediary nature, meaning that they are created or used in the process of creating a subsequent record. To qualify as an intermediary record, the record must also not be required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Records include: non-substantive working files: collected and created materials not coordinated or disseminated outside the unit of origin that do not contain information documenting significant policy development, action, or decision making. These working papers do not result directly in a final product or an approved finished report. Included are such materials as rough notes and calculations and preliminary drafts produced solely for proof reading or internal discussion, reference, or consultation, and associated transmittals, notes, reference, and background materials.

- audio and video recordings of meetings that have been fully transcribed or that were created explicitly for the purpose of creating detailed meeting minutes (once the minutes are created)
- dictation recordings
- input or source records, which agencies create in the routine process of creating, maintaining, updating, or using electronic information systems and which have no value beyond the input or output transaction: o hardcopy input source documents where all information on the document is incorporated in an electronic system (See Exclusion 1 and Note 1) o electronic input source records such as transaction files or intermediate input/output files
- ad hoc reports, including queries on electronic systems, whether used for one-time reference or to create a subsequent report
- data files output from electronic systems, created for the purpose of information sharing or reference (see Exclusion 2)

Exclusion 1: This item does not allow destruction of original hardcopy still pictures, graphic materials or posters, aerial film, maps, plans, charts, sound recordings, motion picture film, or video recordings once they are digitized. Agencies must follow agency-specific schedules for these records. If the records are unscheduled, the agency must submit a schedule for them. Exclusion 2: This item does not include the following data output files (agencies must follow agency-specific schedules for these records, except for the final bullet, which the GRS covers in another schedule):

- files created only for public access purposes
- summarized information from unscheduled electronic records or inaccessible permanent records
- data extracts produced by a process that results in the content of the file being significantly different from the source records.
- In other words, the process effectively creates a new database file significantly different from the original
- data extracts containing Personally Identifiable Information (PII).

Such records require additional tracking and fall under GRS 4.2, item 130 (DAA-GRS-2013-0007-0012). Retention: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. Legal Authority: DAA-GRS-2017-0003-0002 (GRS 05.2/020) GRS 05.3/020 Employee Emergency Contact Information Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers or addresses. Records may also include other information on employees such as

responsibilities assigned to the individual during an emergency situation. Exclusion: This item does not include employee directories that contain information about where employees are located in facilities and work phone numbers. Retention: Temporary. Destroy when superseded or obsolete, or upon separation or transfer of the employee. Legal Authority: DAA-GRS-2016-0004-0002 (GRS 05.3/020)

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.
Yes. The Contractor Information Worksheet includes a Privacy Act Notice in compliance with the Privacy Act of 1974, and as authorized by the Federal Property and Administrative Services Act of 1949. The entire notice states: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of information contained herein may be used as a basis for physical access determinations. GSA describes how your information will be maintained in the Privacy Act system of record notice published in the Federal Register at 73 FR 35690 on June 24, 2008. Your social security number is being requested pursuant to Executive Order 9397. Disclosure of the information by you is voluntary. Failure to provide information requested on this form may result in the government's inability to grant unescorted physical access to GSA-controlled facilities and may affect your prospects for employment or continued employment under a government contract, or at a Federal facility, or with a government license.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
Information collected is necessary to meet:

- The Office of Management and Budget (OMB) Guidance M-05-24 for Homeland Security Presidential Directive (HSPD) 12 which authorizes Federal departments and agencies to ensure that contractors have limited/controlled access to facilities and information systems, and GSA Directive CIO P 2181.1 Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing which states that GSA contractors must undergo a minimum of a FBI National Criminal Information Check (NCIC) to receive unescorted physical access.

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?
To prevent unauthorized access, all GCIMS users must authenticate using an active PIV card and associated PIN. This method ensures the requisite multi-factor authentication model for accessing systems containing PII Sensitive data within the system is encrypted using AES-256 encryption with a protected key or 256-bit hashing. Transport of data is encrypted using SSL and TLS 1.2 the latest secure protocols available.

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

3.4 Explain: Please elaborate as needed.
There is no public access to the system. It is only used to manage GSA employees and contractor personnel. Use of the GSA network and storage devices that maintain GCIMS information is audited in accordance with GSA IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08.

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

The primary reports available in the system are 1.) Complete list of ALL information collected from an individual as requested from the CIW 2.) Summarized totals of information related to adjudications performed on individuals. Reports are provided for the use of OMA and Heads of Service and Staff Offices (HSSOs) personnel to maintain accuracy of system records and financial forecasting and management planning. With few exceptions no reports will not contain PII except SSN/personal email for unique identification purposes when communicating with OPM FSEM.

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?
Reports which do not summarize data using tabular totals will include the names of individuals in the system for the purpose of identification

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?
Federal Agencies

4.2How: If so, how will GSA share the information?
Information is shared with OPM FSEM via the e-QIP application portal and GSA MSO via its USAccess Portal. Both portals use industry standard web browser clients authenticated through PIV cards and HTTPS/TLS communication protocols. The purpose of the sharing is to allow OPM FSEM to conduct the required background investigation on contractors and GSA MSO to produce and issue HSPD-12 PIV cards.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Information is collected from the individual using the Contractor Information Worksheet (OMB Control Number: 3090-0283) or federal employment application forms.

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?
GCIMS interacts with multiple external systems within/outside GSA. For the external agency systems there are MOAs in place and updated on an annual basis. Those include the Managed Service Offering (MSO) and OPM FSEM. Both systems have the proper Security Assessment and Authorization (A&A) from their parent agencies. Please contact the OMA HSPD-12 Office to see the MOA with MSO: Please contact the OMA HSPD-12 Office to see the GCIMS system interconnections document. Please contact the OMA HSPD-12 Office for the agreement with OPM FSEM.

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 GSA HSPD-12 Handbook describes processes to update information in case of employment events for both employees and contractors which in-turn result in an update of personnel data. Also the ICAM Division plans to periodically verify GSA personnel eligibility for GSA Access Card by validating with various Staff and Service Offices. Additionally, the HR system provides a nightly download of all departing employees which helps the data in GCIMS to keep up to date. GSA personnel can also update their "Self Service" information as needed or required. Records with missing information will be flagged as incomplete until missing information is provided. Contract Information Worksheet (CIW) has all required information that is required by GCIMS. Incorrect data can be compared to the CIW for completeness. Business rules are coded into the data fields to determine the accuracy and completeness of inputted data. Twice a year, Point Of Contacts must verify with the HSPD-12 Program Management Office that their personnel records are still up-to-date or provide updates.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?

System information may be accessed and used by: a. GSA Personnel and GSA investigation service provider Office of Personnel Management (OPM) personnel when needed for official use only, including, but not limited to: managing identity information of GSA personnel; managing the issuance and maintenance of Access Cards; and managing the completion of background investigation requirements. b. UiPath robot to download and upload user data files for business processes. GSA personnel assigned to background investigative roles and responsibilities will be authorized to operate the attended robot. The robot operator will have read-write data access to required IT systems which the robot has further restricted programmed usage but not greater than the operator. Robot access and revocation is governed by the GSA Information Technology (IT) Rules of Behavior - CIO 2104.1B (https://www.gsa.gov/cdnstatic/IT_General_Rules_of_Behavior_CIO_21041B_CHGE_1_04-02-2019.pdf) c. To verify suitability of an employee or contractor before granting access to specific resources d. To disclose information to agency staff and administrative offices who may restructure the data for management purposes e. An authoritative source of identities for Active Directory, Google mail, and other GSA systems f. In any legal proceeding, where pertinent, to which GSA is a party before a court or administrative body g. To authorized officials engaged in investigating or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record h. To a Federal, state, local, foreign, or tribal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision i. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes j. To a Member of Congress or staff on behalf of and at the request of the individual who is the subject of the record k. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant l. To the National Archives and Records Administration (NARA) for records management purposes m. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. n. Users who do not have access to personally identifiable information data are: o IT Helpdesk Personnel o Building Managers controlling physical access o System Administrators providing logical access o Record holders updating their personal information (Employment Information, Emergency Contacts, Work and Home Address) in the self-service module. o Google Mail Team

6.1b: What is the authorization process to gain access?

All individuals who have been issued a GSA PIV card can access their records using the GCIMS website

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.
9/30/2016

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
[Indicate the types of physical barriers that protect the information (security guards, identification badges, key cards, safes, locks, etc.). Indicate the types of technical protections for the information (user identification, password, encryption, multi-factor authentication, etc.). GSA requires encryption of sensitive PII, PCI, and user-credential information. This includes encryption of the data in any form including in transit, at rest, and file database level encryption. List examples of administrative controls (periodic security audits, regular monitoring of users, backup of sensitive data, etc.).]

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?
GSA has procedures in place for handling security incidents. GSA monitors use of its systems and is responsible for reporting any potential incidents directly to the relevant Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
All forms requesting information include a Privacy Act Notice in compliance with the Privacy Act of 1974, and as authorized by the Federal Property and Administrative Services Act of 1949. The entire notice states: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of information contained herein may be used as a basis for physical access determinations. GSA describes how your information will be maintained in the Privacy Act system of record notice published in the Federal Register at 73 FR 35690 on June 24, 2008. Your social security number is being requested pursuant to Executive Order 9397. Disclosure of the information by you is voluntary. Failure to provide information requested on this form may result in the government's inability to grant unescorted physical access to GSA-controlled facilities and may affect your prospects for employment or continued employment under a government contract, or at a Federal facility, or with a government license.

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.
No opportunity exist to consent, decline or opt-out.

7.2: What are the procedures that allow individuals to access their information?
All individuals who have been issued a GSA PIV card can access their records using the GCIMS website. For all others, the HSPD-12 help desk has a phone number that can be contacted to request information on individuals.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Individuals who wish to amend information about themselves must contact the Office of Personnel Management through an email or the office phone number.

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.
GSA requires annual privacy and security training for all personnel and has policies in place that govern the proper handling of PII. This is managed through the CIO and Online Learning University system.

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?

GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. Further, OMB requires the GSA to document these privacy protections in submissions for Information Collection Requests processed under the Paperwork Reduction Act. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately. As discussed above, GSA takes automated precautions against overly open access controls