GSA Credential & Identity Management System (GCIMS)

Privacy Impact Assessment (PIA)

April 5, 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):

- Nate Ciano

Name of Program Manager/System Owner:

- Phillip S. Ahn

Signature Page

Signed:

DocuSigned by:
Nathaniel Ciano
113E72276281433...
Information System Security Manager (ISSM)

DocuSigned by:
Phillip Ahn
1A4B294315ED445...
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.

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 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 *GSA Credential and Identity Management System (GCIMS).* To accomplish its mission *Office of Mission Assurance* must, in the course of *HSPD-12 Security PMO,* 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:

GSA Credential and Identity Management System (GCIMS) of Enterprise Application Services (EAS) FISMA system.

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:

The system contains information needed for issuing and maintaining HSPD-12 credentials with the Managed Service Offering (MSO) and also access privilege information. Records may include:

- *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:*
    - *Port of entry city and state*
    - *Date of entry*
    - *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:*
    - *Contract company (also referred as vendor)*
    - *Vendor Point of Contact (POC)*
    - *Whether contract company is the prime or a subcontractor*
    - *Name of prime if company is subcontractor*
    - *Task order number, delivery order, or contract base number*
    - *Contract start and end date*

- *Contract option years (yes or no)*
- *Names of previous companies on GSA contracts*

Overview

The GCIMS application is the system for managing all credentials issued to GSA personnel and GSA contractors and background investigation processes. Anyone who has a GSA PIV has information stored in GCIMS. GSA personnel information is imported from the GSA HR system and contractor information is manually entered from Contractor Information Worksheets (CIWs). GCIMS submits and retrieves information from the Managed System Operations (MSO) via a web service.

GSA contractors can login to the system to update their personal information. GSA personnel with credentialing management responsibilities initiate and track applicant credentialing requests. The application provides search capabilities for organization, contract, and person. A credential screen summarizes the employee/contractor's personal information, status, issued credential, and investigation status. GCIMS enables a user to track important dates in the credentialing process. The system diagram below shows the interaction between GCIMS and MSO systems. The connection to HR is established to synchronize authoritative GCIMS attributes with that system. GCIMS is the critical application that serves the credential data to MSO systems. GCIMS information is also distributed to Active Directory, the Insite Staff Database, and the National Alert and Accountability System (NAAS).

PII is collected such as DOB, SSN, gender, addresses, birth place, etc. related to an individual to identify the individual and contact them as part of the background check processing by OPM FSEM and credentialing by the MSO. In addition, related information is requested to tie contractors to GSA contracts, buildings, and vendor POC information to allow notification of applicants concerning HSPD-12 compliance and initial/final adjudication determinations.

RPA BOT Process:

An attended Bot navigates to the GSA Credential & Identity Management System (GCIMS) and downloads files containing information on GSA Contractors that are requesting security clearances.

The files from GCIMS are downloaded to a temporary folder and then uploaded to e-QIP. The files include each contractor's SSN, Full Name, Place of Birth, Email, and Phone #. These files are then uploaded to the Office of Personnel Management's (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) site to request investigations for the GSA contractors.

Once the upload process has completed, all files are deleted. The Bot does not maintain or collect the process custodian's user IDs and passwords as the custodian must log into GCIMS and e-QIP before running the bot.

The e-QIP Mass Invite process is performed in three stages: downloading files from GCIMS; uploading files into e-QIP; and verifying data in e-QIP. This process happens 6 times a day, 5 days a week. When GCIMS creates files for e-QIP Mass Invite process, GCIMS identifies all GSA contractors that need a background investigation. Files are separated by the type of investigation needed for each contractor. Files will identify anyone that has requested that type of investigation since the previous run of the downloading process. After the GCIMS files are downloaded, the Bot uploads them into e-QIP. While uploading each file, the type of investigation determines selections of AUB (Agency Use Block) and other requirements in e-QIP. Once all the files are uploaded, staff verify that the data in GCIMS has been updated in e-QIP.

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?

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? If so, what System of Records Notice(s) apply/applies to the information?

Yes, 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.

1.3 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.

Yes, the Supporting Statement for Information Collection Submission OMB Control Number 3090-0283.

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.

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)

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.

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.

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?

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

No.

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?

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

No. Reports which do not summarize data using tabular totals will include the names of individuals in the system for the purpose of identification.

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. Because the HSPD-12 program manages the background investigation of contractors, it has a requirement to access a large category of information to adequately determine an individual's trustworthiness for a particular job function. The collected data is not shared with persons or offices outside the Inspector General that do not have a role in this investigation or HSPD-12 process.

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 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 or is it taken from another source? If so, 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? If so, who and how? Is a formal agreement(s) in place?

Yes, 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.

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 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.

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?

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:

- *IT Helpdesk Personnel*
- *Building Managers controlling physical access*
- *System Administrators providing logical access*
- *Record holders updating their personal information (Employment Information, Emergency Contacts, Work and Home Address) in the self-service module.*
- *Google Mail Team*

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

Yes, GSA has completed system security plans (SSPs) for the systems that support and maintain the information used in GCIMS. GSA categorizes all of its systems using Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). GCIMS operates on systems rated "moderate impact." Based on this categorization, GSA implements security controls from NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" to secure its systems and data. This was last authorized in 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? If so, 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.

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.

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.

7.2 What procedures 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? If so, how?

The HSPD-12 help desk has a phone number that can be contacted to request information be corrected or updated on individuals.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

GSA has developed, implemented, and regularly updates its IT Security Awareness and Privacy Training as part of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities.

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.

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?

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.

---

[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.