GSA Credential and Identity Management System (GCIMS)

Privacy Impact Assessment

November 2, 2018

POINT *of* CONTACT

Phillip Ahn

HSPD-12 Program Manager

GSA Office of Mission Assurance

1800 F Street, NW

Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses 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 demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

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. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:
https://www.gsa.gov/portal/getMediaData?mediaId=167954

If you have any questions, send them to gsa.privacyact@gsa.gov.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Revised to include questions about third party services on websites and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding "Information Collection Requests"	2.1

Table of contents

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 the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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 for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline 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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about *GSA Credential and Identity Management System. Office of Mission Assurance* may, in the course of *HSPD-12*, 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

GSA Credential and Identity Management System (GCIMS)

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, to whom GSA facilities may issue local Facility Access Cards (FAC).

System, application or project includes

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 cardholders 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, and also generate and print hard or soft

copies of the Contractor Information Worksheet (CIW), using the applicant's data in the system. 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 FSC 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.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

The primary purposes of the system are:

To act as an authoritative source for GSA identities including employees and contractors to verify that all persons requiring routine access to GSA facilities or using GSA information resources have sufficient background investigations and are permitted access, to track and manage PIV smart cards issued to persons who have routine access to GSA facilities and information systems, to provide reports of identity data for administrative and staff offices to efficiently manage personnel, and to track and process background investigations for GSA personnel. (GSA branded the PIV card that it issues to its personnel as the GSA Access Card.)

1.2 What legal authority and/or agreements allow GSA to collect 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).

1.3 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 being collected?

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

1.4. Has any 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.

1.5. 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.

Records are maintained and verified while an employee has active employment status at GSA following a 2 year schedule. Records are disposed of as specified in the handbook, GSA Records Maintenance and Disposition System (CIO P 1820.1). The record retention period is indefinite due to the continual re-application of contract staff at GSA and the need to review previous background investigation results for HSPD-12 and OMB reporting compliance.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

There are no identified potential effects on the privacy rights of individuals. Risk is mitigated because no new data is derived from the original data and also existing, proven web technologies are used in building this federal system. Also, GCIMS does not provide decision making capabilities, but only acts as a personnel management system and authoritative data source.

As users are the ones that can potentially cause inadvertent sharing of information, it is the responsibility of the user to only share such information as required, on a need to know basis and only for the specified period required to support mission functions. Controls have been put in place to prevent users from inadvertently sharing information with all members of the organization.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing 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.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Yes, the openness and transparency requirement labels the information system as a high-value target for data theft through phishing and digital intrusion. To mitigate the risk, the system is monitored, audited, and protected according to GSA IT policies and NIST requirements for IT systems.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII 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 Whose information is included in the system, application or project?

a. Federal employees.
b. Contractors.

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

3.2 What PII will the system, application or project include?

The system contains information needed for issuing and maintaining HSPD-12 credentials with the 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
- 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

Full 9-digit SSNs are collected because it is required by OPM FSC to perform its background investigation activities within credit bureau and criminal database searches and uniquely identifies individuals in their system of record.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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/FAS 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 FSC.

3.8 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

No.

SECTION 4.0 LIMITS ON USES AND SHARING OF 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 FSC 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 FSC 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, how and 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 annual basis. Those include the Managed Service Offering (MSO) and OPM FSC. Both systems have the proper Security Assessment and Authorization ("A&A") from their parent agencies.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Yes, there are inherent privacy risks with sharing PII with external systems. Users are notified on forms where data is collected on the business purpose but not specifically how the data will be secured.

GSA outlines appropriate uses and access controls for PII whenever it enters into agreements with third parties; for example, through data-sharing agreements, MOAs, or contracts. GSA does verify that their shared systems operate under the same NIST standards that our own platforms must be certified and compliant.

In addition, a suite of automated tools are used to scan the systems for the latest known security vulnerabilities and provide follow up for mitigation. Encryption is a critical piece of the security posture and is updated or upgraded as older protocols are sunset.

Whenever possible, software code is used to replace humans when processing data to minimize the leakage of PII. The goal is to refine and remove access to PII to the

greatest extent possible while still balancing business efficiencies and customer responsiveness.

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 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.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

There are no additional privacy risks related to data quality and integrity. However, GCIMS does attempt to mitigate unforeseen issues by classifying users into different categories. These classifications support the technical control concepts of Separation of Duties, Least Privilege, and Accountability. Each category of user has a distinct set of roles and responsibilities that determine the information to which they have access and the actions they are permitted to perform. The access to data by a user is determined based on the GSA's HSPD-12 Handbook which contains standard operating procedure

for background investigation and credentialing GSA personnel. Users must meet background investigation and training requirements in addition to signed approval from their regional/departmental authorizing official prior to gaining access to GCIMS.

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; managing the completion of background investigation requirements.

Additional users who do not have access to privacy 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

b. To verify suitability of an employee or contractor before granting access to specific resources;

c. To disclose information to agency staff and administrative offices who may restructure the data for management purposes;

d. An authoritative source of identities for Active Directory, Google mail, and other GSA systems;

e. In any legal proceeding, where pertinent, to which GSA is a party before a court or administrative body;

f. To authorized officials engaged in investigating or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record.

g. 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;

h. 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;

i. To a Member of Congress or staff on behalf of and at the request of the individual who is the subject of the record;

j. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant;

k. To the National Archives and Records Administration (NARA) for records management purposes;

l. 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.

6.2 Has GSA completed a system security plan 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.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

GSA assesses information and systems for compliance risk, reputational risk, strategic risk, situational/circumstantial risk, and operational risk. In order to mitigate these risks to an acceptable level, GSA implements extensive security controls for information collected or maintained on its behalf, and conducts third-party assessments of vendors and services it procures.

GSA implements the following controls for internally maintained systems: GSA policies and procedures governing privacy and information security; background checks on all personnel with access to the system; initial and follow-on privacy and security awareness training for each individual with access to the system; physical perimeter security safeguards; Security Operations Center (SOC) to monitor antivirus and intrusion detection software; risk and controls assessments and mitigation; technical access controls, such as role-based access management and firewalls; and appropriate disaster mitigation strategies, breach notification processes and plans, and secure channels for submitting information.

GSA implements controls relevant to third party vendors and services according to risks identified the following types of third party reviews: Third Party Security Assessment and Authorization (SA&A) Package; Statements on Standards for Attestation Engagements (SSAE) Review; Risk Assessments by Independent Organization; or a complete Risk Assessment by GSA.

6.4 Are there mechanisms in place to identify 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls.

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 are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline 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.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Individuals are allowed through self-service functions to update their information but not allowed to delete or remove their record. Separation of duties provides safeguards against irreparable changes to individual records.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

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.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

Yes. All GSA personnel granted HSPD-12 roles are made aware of the potential risks inherent in using GCIMS through activities including but not limited to, monthly user group meetings, email reminders, and the publication of this PIA.

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, application or project ensure that the information is used in accordance with 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.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes, persons performing accountability and auditing will have elevated privileges in the system.

To mitigate this risk, GSA clearly identifies personnel with the capacity to audit GCIMS and provides them with appropriate role-based training. Auditors perform their duties in collaboration with GSA supervisors and/or GSA's Privacy Office. In addition, access to PII information is curtailed or aggregated as needed for the specific purpose of the audit being performed.

---

[1] OMB Memorandum *Preparing for and Responding to a 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.