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: 385
System Name: Enterprise Infrastructure Operations (EIO)
CPO Approval Date: 6/16/2022
PIA Expiration Date: 6/15/2025

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:
Enterprise Infrastructure Operations (EIO)

B: System, application, or project includes information about:
Federal employees and contractors

C: For the categories listed above, how many records are there for each?
We are unable to make a determination on the number of records contained within the digital storage. Active Directory holds 25,593 active and inactive accounts (including service accounts).

D: System, application, or project includes these data elements:
Active Directory has potential to hold data from within the following categories . Name . Contact Information (e.g., GSA telephone number/GSA email address) . Other Information (including mobile device number: GSA provided or personal (if BYOD)) . See table below for more detailed information

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 11315, 44 U.S.C. 3506, 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?
the information contained within the GSS is covered by existing SORNs: . GSA/CIO-1 GSA Credential & Identity Mgmt System (GCIMS) . GSA/CIO-2 Enterprise Server Services . GSA/CIO-3 GSA Enterprise Organization of Google Applications and SalesForce.com . GSA/HRO-37 Security Files (HSPD-12 System) (Exempt) . GSA-OMA-1 E-PACS

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
No record retention schedule has been approved by NARA. There is no known physical documentation or records containing PII for Active Directory. The only records would be contained within the backups for Active Directory, which are maintained for one year. The data within Active Directory is stored within Active Directory as long as the individual is employed by GSA. Once an individual is no longer employed by GSA, as part of the off-boarding process, the AD account is placed in the NetIQ-DRA recycle bin for 180 days. After 180 days, the user account is permanently deleted from the Net-IQ DRA recycle bin.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.
There will be no notice given since the information contained within AD is imported from GCIMS. Any notice would be provided from GCIMS.

3.0 Data Minimization

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

The information is collected, used, maintained and disseminated to enable effective, reliable and secure operation of the IT network to support GSA's mission and daily operations. Much of the PII processed on or transiting through the GSS is collected, used, disseminated and maintained for the functioning and security of the IT network. Because the GSS forms the IT network infrastructure and other GSA major and minor applications reside on or link to the GSS, PII from those other applications can be processed on or transit through the GSS. Examples of the more specific purposes of PII collection, use, maintenance and dissemination include to: add and delete network users, i.e., enable GSA employees, interns, volunteers, contractors and consultants to access the IT network and components (e.g., workstations and mobile devices), and when no longer working for the GSA, to disable their access; enable network users to securely connect, store, and access data within other GSA applications; monitor usage of and security of network components and applications; ensure the availability and reliability of the GSA network components and applications; document and/or control access to various network applications; audit, log, and alert responsible GSA personnel when certain PII is accessed in specified systems; investigate and make referrals for disciplinary or other action if improper or unauthorized use is suspected or detected; enable electronic communications between GSA network users, and to and from GSA network users with individuals outside the GSA.

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?
The information in the GSS is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. For example, all access to the GSS is on-site or via a secured virtual private network (VPN) connection. Also, GSA staff regularly review GSS audit records for indications of inappropriate or unusual activity.

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

3.4 Explain: Please elaborate as needed.
No, the system does not provide the capability to monitor an individual in real-time. However, the GSS: 1) Can confirm whether an individual is logging into the GSA network from a GSA desktop as opposed to a remote computer via VPN. 2) Contains mobile device management software that allows specifically designated GSA IT staff to locate a GSA mobile device, if such a device is lost or stolen 3) Includes PIV card activity information, including time and GSA office location of use by card holder

3.5 What kinds of report(s) can be produced on individuals?
User activity reports can be produced.

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?
Custom reports can be generated from AD where only specific fields of data can be selected as needed per request. There are no standard or regular reports generated that would contain PII. Therefore, reports will not be de-identified, they will include PII if needed, and not shared outside of GSA, unless authorized by law.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
GSA maintains policies and processes to restrict access to the GSS internally to those network users who have a need to know the information to perform their job duties. GSA contractors with access to the GSS, including information security specialists, are required to comply with the Privacy Act and GSA information usage policies and procedures contractually through either Federal Acquisition Regulation (FAR) terms or other terms and conditions. Many contractors also individually sign non-disclosure agreements. Any Active Directory report that would need to be shared inside or outside of GSA containing PII, would be done so by email, where the report is encrypted in a password protected zip file, per GSA policy.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
The sources of information contained in the GSS are current and former GSA IT network users, including current and former employees, interns, volunteers, contractors and consultants; information from other GSA major and minor applications that is processed on or through the GSS, e.g., information from market and oversight, civil law enforcement and internal administrative applications, and from applications through which registrants and other individuals submit information; and GSA hardware, software and system components that generate information reflecting activity on the GSA IT network. For example: GSA network user information needed for the GSS and its components to operate efficiently and securely and for the GSA to control access to software, applications, data and information; activity logs, audit trails, identification of devices used to access GSA systems, 14 Version 3.3: April 02, 2020 Internet sites visited, and information input into sites visited; logs of calls to and from a GSA network user on desk or mobile phones, and similar communication data traffic logs; records of the name of authorized GSA users, PIV card identifiers, user access level, and status (e.g. active/inactive), also including PIV card activity information, including time and GSA office location of use by card holder; and including but not limited to information stored in internal collaboration tools.

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?
The GSS forms the IT network infrastructure; the GSS, by itself, does not automatically collect or share data outside GSA, i.e., there are no interconnections with external systems that would result in automated sharing data. However, there are certain other GSA major and minor applications within their own FISMA boundary that may send information using methods such as secure file transfer (SFTP) that crosses through perimeter devices such as switches, routers, and firewalls, which fall within the EIO GSS boundary. Formal agreements would fall under the FISMA systems of those major and minor applications. Formal agreements are not required within GSA between FISMA boundaries.

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

4.4NoAgreement: Why is there not a formal agreement in place?
Formal agreements would fall under the FISMA systems of those major and minor applications. Formal agreements are not required within GSA between FISMA boundaries.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
Each network user is responsible for the accuracy of the information entered into or transmitted by the GSS. The data owners are responsible for the accuracy and completeness of all information collected for their applications. ISSOs do not have access to application data. GSA performs many relationship edits and data checks to ensure data entered is as accurate as possible. Fields are defined in the database to ensure valid data. Users are assigned specific accounts for update and not allowed access to all employees in the system. GSA roles ensure separation of duties to prevent anomalies and fraud.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Data access is restricted with the use of roles and permissions within the GSS. GSS employees are instructed to not update their own data.

6.1b: What is the authorization process to gain access?
Data access is restricted with the use of roles and permissions within the GSS. GSS employees are instructed to not update their own data.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
10/31/2019

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The information in the GSS is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. For example, all access to the GSS is on-site or via a secured virtual private network (VPN) connection. Also, GSA staff regularly review GSS audit records for indications of inappropriate or unusual activity.

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?
EIO leverages the GSA Incident Response (IR) guide. In case of a suspected security incident/breach of PII, the IT Service Desk as well the Privacy Office and Incident Response team are notified immediately to start investigations.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Since AD imports data from GCIMS, any individual's ability to consent or decline to provide information would have to be through GCIMS. Only Active Directory admins are allowed access to the data within Active Directory for security purposes. Access to correct or amend would need to be through GCIMS.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Since AD imports data from GCIMS, any individual's ability to consent or decline to provide information would have to be through GCIMS. Only Active Directory admins are allowed access to the data within Active Directory for security purposes. Access to correct or amend would need to be through GCIMS.

7.2: What are the procedures that allow individuals to access their information?
Users are only able to access their information if they have access to GCIMS. Only designated Directory Services administrators have access to Active Directory. GCIMS is not part of the EIO FISMA system.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Users are only able to amend their information if they have access to GCIMS. Only designated Directory Services administrators have access to Active Directory. GCIMS is not part of the EIO FISMA system.

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
All GSA employees and contractors are required to take the IT Security Awareness and Privacy 101, Privacy 201 training, and Sharing in a Collaborative Environment training annually. The Rules of Behavior is included in the required security training and policies in place that govern the proper handling of PII.

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. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately.