



Enterprise Infrastructure Operations (EIO)

Privacy Impact Assessment (PIA)

April 20, 2020

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):

- Matthew Regan

Name of Program Manager/System Owner:


- David Harrity


Signature Page

Signed:

DocuSigned by:

92526A8616CB470...
Information System Security Manager (ISSM)

DocuSigned by:

6EA69AEB1ED048E...
Program Manager/System Owner

DocuSigned by:

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.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

3-20-2020	Completed ISSO updates	3.2
04-02-2020	Final Update Completed	3.3

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 the Enterprise Infrastructure Operations (EIO) FISMA System. To accomplish its mission GSA IT provides digital storage and creates accounts within Active Directory (AD). For AD, personally identifiable information (PII) about the people who will have access to the GSA network is imported from the GSA Credential Identity Management System (GCIMS) system, which is part of the EAS FISMA boundary. 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:

Enterprise Infrastructure Operations (EIO) FISMA system

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 17,792 active and inactive 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

Active Directory imports data directly from GCIMS with the following fields that may contain PII:

GCIMS Management Agent	MIM Metaverse	Addressbook.GSA.GOV (ADLDS)	ENT (Active Directory Domain)	EXT (Active Directory Domain)	DSDATA (SQL DB)
Contact_ID	GCIMS-ContactID	ContactID			
Pers_Cotr_Email	PersCotrEmail	PersCotrEmail			
Pers_Cotr_Name	PersCotrName	PersCotrName			
pers_emp_id	EmployeeID	EmployeeID			
pers_name_cordial	CordialName	GivenName	GivenName	GivenName	CordialName
pers_name_family	LastName	sn	sn	sn	LastName
pers_name_given	FirstName				FirstName
pers_name_middle	MiddleName		MiddleName	MiddleName	MiddleName
pers_upn	LoginName; GCIMS_UPN	UserPrincipal Name	UserPrincipal Name		
pers_work_bpb_pin	pager	otherPager	otherPager		
pers_work_cell	MobilePhone	Mobile	Mobile		MobilePhone
pers_work_email	email	mail	mail	mail	email
pers_work_fax	officefax	facsimileTelephoneNumber	facsimileTelephoneNumber		fax
pers_work_phone	officephone	telephoneNu	telephoneNu	telephoneNu	officephone

hone		mber	mber	mber	
pers_affiliation; pers_name;pers_office_symbol	googleMailSurname				

Data is not directly entered into Active Directory, as stated above it is pulled from GCIMS, except for the AD ENT or EXT account name, which is created within Active Directory by mid-tier support and is synced to EXT is required.

Overview

Enterprise Infrastructure Operations (EIO) is a GSA General Support System (GSS) that encompasses the server, identity management, database management, network, security and client enterprise infrastructures. EIO is responsible for designing, implementing, managing, and maintaining the server and storage enterprise infrastructure that includes on-prem physical, on-prem virtual, and in the AWS cloud (BigFix relays), along with the AAA (Authentication, Authorization, and Auditing) identity management infrastructure via Microsoft’s Active Directory, SecureAuth, and Single SignOn. EIO consolidates service offerings for database and middleware management to provide a Single Source resource for Business Line Database and Middleware Solutions.

Additionally, EIO is responsible for desktop management which includes patching, configuration, and hardening. Providing virtual client platforms, mobile device management relating to the security management of mobile devices, local support which consists of on-site support services to the Service and Staff Offices of GSA, and the Enterprise IT Service Desk (EITSD) which is a single point of contact for all IT infrastructure issues across the GSA enterprise and is the front line of support for all GSA employees on a 24/7/365 basis.

The main components of the infrastructure include:

- Client devices
- Servers
- WAN
- MAN
- LANs
- Virtual Networks
- Network Perimeter Devices and Boundary Protections

- Remote Access Devices
- Active Directory
- File and Print Servers
- Database and Middleware Management Systems
- Identity, Credentialing, and Access Control Management Systems

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?

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

Yes, 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

1.3 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.

No

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.

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.

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.

There will be no notice given since the information contained within AD is imported from GCIMS. Any notice would be provided from GCIMS.

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?

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? 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?

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?

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

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.

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

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?

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 directly from the individual or is it taken from another source? If so, 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,

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? If so, who and how? Is a formal agreement(s) in place?

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.

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?

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.

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?**

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

Yes, the SSP was last updated in October 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? If so, 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.

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.

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 procedures 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? If so, how?

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.

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.

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.

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

^[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.