



Enterprise Application Services (EAS)

Privacy Impact Assessment (PIA)

8-10-2020

POINT of CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Stakeholders

Name of Information System Security Manager (ISSM):

- Nathaniel Ciano

Name of Program Manager/System Owner:

- Chris McFerren

Signature Page

Signed:

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

DocuSigned by:
Chris McFerren
2084003077FB404...
Program Manager/System Owner

DocuSigned by:
Richard Spidel
174D6411482F40A...
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
7-13-2020	Updated 2019 Version	1.0
8-4-2020	Added Document Revision History	2.0
8-5-2020	Updated numbering	3.0
8-10-2020	Concur with ISP	4.0

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 to 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 Enterprise Application Services (EAS). To accomplish its mission, GSA IT must, in the course of providing an email solution, document management functionality, financial/HR reporting capabilities, and personnel adjudication tracking data, collect and/or process 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:

Enterprise Application Services (EAS)

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?

This is the overarching PIA for EAS; therefore in order to view the number of records for each subsystem that contains PII, please visit <https://gsa.gov/pia> to view the application specific PIA.

D. System, application, or project includes these data elements:

The following EAS subsystems contain Personally Identifiable Information (PII). This PIA template has been truncated since PIAs exist for the five (5) systems below; therefore, please visit www.gsa.gov/PIA for the latest versions of each.

1. GSA Credential Information Management System (GCIMS)
2. Office of Civil Rights (OCR) Complaint Management System (OCR-CMS)
3. GSA Security Tracking and Adjudication Record System (GSTARS)
4. Google (G) Suite
5. Electronic Document Management Software (EDMS)

A summary is provided below for each application describing the PII that is being collected.

1. **GSA Credential Information Management System (GCIMS):** The GCIMS application is designed to track GSA employee and contractor status in the credentialing and background investigation processes. GSA management, users, and respective role-holders will have the ability to record the initiation of a PIV card request for a particular applicant, as per the HSPD-12 and GSA specific requirements and procedures, manage the person's organization/company and/or contract affiliation, as well as the overall credentialing and investigation status during the process progression. The application provides search capabilities for organization, contract, and person. A credential screen summarizes the employee/contractor's personal information, status, issued credential, and conducted investigation. GCIMS enables a user to track important dates in the credentialing process, and also generate and print hard or soft copies of the Contractor Information Worksheet (CIW), using the applicant's data in the system. Please refer to the GCIMS PIA.
2. **Office of Civil Rights Complaint Management System (OCR-CMS):** OCR utilizes the Complaint Management System to: (1) file complaints and receive updates on their EEO cases (efile module); (2) monitor and track complaints nationwide; and (3) report on nationwide complaints activity including reports to EEOC (No FEAR and QRM modules). As per a congressional requirement, agencies must submit annual reports to the EEOC and to Congress, and must purchase and/or develop systems that can compile the necessary information to track EEO complaint activity for case management and reporting as set forth in EEOC regulations. Please refer to the OCR-CMS PIA with EAS A&A package.
3. **GSA Security Tracking and Adjudication Record System (GSTARS):** The Personnel Security Branch Case Management System automates the tracking of personnel security investigation activities for the General Services Administration (GSA). The purpose of GSA Security Tracking and Adjudication Record System (GSTARS) is to enable the GSA Office of Mission Assurance, Personnel Security Division, and Personnel Security Branch to store and manage GSA personnel security information. In addition, GSTARS will allow Personnel Security to manage the integrated workflow process, management activities, caseloads, and reporting capabilities relating to personnel security investigations. Information contained within GSTARS includes: pre-employment waivers, background investigations (BIs), security clearances, SCI access, clearance receipts (reciprocity), reinvestigations, completion dates of various security checks, and adjudication status. Other information contained within GSTARS may include adjudication notes, decisions, employment records, education history, credit history, the subject's previous addresses, friends and associates, selective service records, military history, and citizenship. The personally identifiable information (PII) collected consists of data elements necessary to identify the individual and to track completion of security related processes including background or other investigations concerning the individual. The system has been designed to closely align with the Personnel Security Branch business practices, collecting and maintaining personally identifiable information which may be developed during the security investigation. Please refer to the GSTAR PIA with EAS A&A package.
4. **G Suite:** G Suite is a collection of online messaging and collaboration applications offered as a Software as-a-Service (SaaS) in a cloud computing environment. There are 37 minor Google Applications (Apps) that have been integrated within the GSA infrastructure to provide communication and collaboration services. G Suite core apps (primarily Email, Sites, Groups and Docs) may contain PII stored there by users for the purposes of normal day to day work operations, collaboration or simple storage. None of these apps collects that information as part of the processes. Sources may vary widely as information is not collected by the system's

applications specifically, but are used as a mechanism to store, collaborate and share information between users. The potential PII stored and shared using G Suite comes from a varied source of extracts and sources. Its primary purpose for being in G Suite is either for storage, sharing or collaboration. Please refer to the G Suite PIA with EAS A&A package.

5. **Electronic Document Management Software (EDMS):** The purpose of the Electronic Document Management Software (EDMS) system is to serve as a repository for GSA documents to reduce paper storage and provide reliable and secure access to documents where and when they are needed. The information system also allows for Enterprise document management and records management functionality. Currently, EDMS is migrating content from the PBC Enterprise Content Management System (ECMS) system into the EDMS boundary and the ECMS content owner has identified possible PII data elements that could be embedded within the corpus of the data. Data elements include, but are not limited to Full Names, Place of Birth, Date of Birth, Home Address, Phone Numbers, Email Address, Taxpayer Identification Number (TIN), and Driver's License Number.

The below subsystems of EAS do not have PIAs; therefore a separate PTA has been completed for each.

- Financial Data Reporting System (FDRS)
- Salesforce via force.com (EEO, PEO, GEO, PD, CEO, Client Solutions and Workspaces Orgs)
- Google Cloud Platform (GCP)
- ServiceNow
- MaaS360
- Decision Lens
- Cloudlock
- Apptio TBM
- Qualtrics
- Everbridge Notification and Alert System
- DocuSign Federal
- Workiva
- Geometrics
- GEAR
- GSA Web services (Listsrv, SFTP, GSA Blogs, Bookit, Apex-redirect)
- Zoom
- Slack

Overview

The GSA Enterprise Application Services (EAS) system is operated by the Office of Corporate IT Services, GSA OMA & other IT Offices. EAS is a GSA GSS with on premises hosted and vendor (FedRAMP) hosted applications and it is comprised of two major components Enterprise Ancillary Application (EAA) & Enterprise Cloud Services (ECS). These applications are used to provide services to the GSA Enterprise and the public user community. The authorization boundary includes the EAS on premises applications as well as cloud technology which are approved by FedRAMP. GSA's Associate Chief Information Officer of the Office of Corporate IT Services is the Authorizing Official of EAS and all the minor applications that fall under this system.

The ECS subcomponents are responsible for implementing the required NIST 800-53 controls shared by both the cloud vendors and GSA. The vendor is responsible for implementing the majority of NIST 800-53 security controls while GSA is responsible for implementing those identified as “customer configurable controls” outlined in the section “Overall Control Status”. Additionally, GSA cloud applications inherit authentication, authorization and audit (AAA) security controls (but then have to be locally implemented) from GSA’s Active Directory infrastructure via the GSA Enterprise Infrastructure Operation system.

This PIA template has been truncated since PIAs exist for the five (5) systems mentioned above that comprise EAS. Therefore, please visit www.gsa.gov/PIA for the latest versions of each.