Enterprise Application Services (EAS)

Privacy Impact Assessment

28 MAY 2019

POINT *of* CONTACT

Richard Speidel

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

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 the Enterprise Application Services FISMA system's-IT may, in the course of providing email solution, emergency notification collect. Onboarding system 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

Enterprise Application Services (EAS)

System, application or project includes information about

Federal employees and contractors

System, application or project includes:

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

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.

ECS sub components is responsible for implementing the required NIST 800-53 controls is 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 in 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 GSA Enterprise Infrastructure Operation system.

The following are the applications within EAS that contain data subject to the Privacy Act (Personally Identifiable Information – PII). The summary of each application describes the PII data that is 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) provide for complainants to file complaints and receive updates on their case (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 congressional requirement

agencies must submit annual reports to the EEOC and to Congress, and they 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. Collects and maintains the following 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.

The following subsystems of EAS do not have PIAs. A separate PTA has been completed for each of the subsystems below.

1. Web Services - Comprised of SFTP, Hydra web services, BookIt, Listserv
2. GSA EA Analytics and Reporting (GEAR)
3. Electronic Document Management Software (EDMS)
4. FDRS - a.k.a. SAP Business Objects XI R4-PTA
5. Salesforce customer engagement (CEO)
6. Salesforce CEO org - customer management
7. Salesforce CEO org - case management
8. ServiceNow
9. Mass360
10. E-Sign live
11. Decision Lens

This PIA template has been truncated since PIAs exist for the four aforementioned systems that comprise EAS. Therefore, please visit www.gsa.gov/PIA for the latest versions of each.