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: 374
System Name: GSA Security Tracking and Adjudication Record System (GSTARS)
CPO Approval Date: 5/9/2022
PIA Expiration Date: 5/8/2025

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Security Tracking and Adjudication Record System (GSTARS)

B: System, application, or project includes information about:
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, including but is not limited to:

- Full Name
- Social Security No.
- Citizenship Status
- fingerprint results
- email address
- Date of Birth
- Place of Birth
- Gender
- Organizational and Employee affiliations, Medical History
- Criminal History
- Mother's Maiden Name
- Employment History
- Credit History
- Phone Numbers
- Position Title
- Position Sensitivity
- Eligibility Level Clearance / Eligibility Date / Adjudication Date
- Clearance Type: Secret, Top Secret, SCI
- Reports of Foreign Travel
- Reports of foreign contacts
- Security Incident Reporting
- Background Investigative Reports
- Nondisclosure Agreements
- and Requests for access to Sensitive Compartmented Information (SCI).

C: For the categories listed above, how many records are there for each?
Currently, there are approximately 6605 unique records in GSTARS, and new records are added daily.

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

- Full Name, Social Security Number, Citizenship Status, fingerprint results, email address, Date of Birth, Place of Birth, Gender, Organizational and Employee affiliations, Criminal History, Mother's Maiden Name, Employment History, Credit Reports, Phone Numbers, Position Title, Position Sensitivity Eligibility Level Clearance / Eligibility Date / Adjudication Date
- Clearance Type: Secret, Top Secret, SCI

- Reports of Foreign Travel
- Reports of foreign contacts
- Security Incident Reporting
- Background Investigative Reports
- Nondisclosure Agreements
- and Requests for access to Sensitive Compartmented Information (SCI); and other government-issued identifiers or images of documents, etc.; as part of the background investigation process.

Overview:

The GSA Security Tracking and Adjudication Record System (GSTARS) leverages Micropact's Entellitrak Software as a Software as a Service (SaaS) solution that enables GSA Personnel Security Branch to manage the personnel security clearance and investigations program. This system will serve to streamline and integrate its various personnel security program requirements and generate timely metrics to measure Personnel Security Branch (D1SB) performance. GSTARS will allow D1SB to take steps to reduce the amount of paper used in the clearance process by becoming paperless and to maintain records electronically as required by the Government Paperwork Elimination Act (GPEA). The new Case Management System will also assist D1SB in meeting deadlines set forth in the National Intelligence Reform Act of 2004.

The Entellitrak BI Integration Application will be integrated with the OPM PIPS Daily Case Status by automatically importing files, containing case information for all the cases processed by OPM, on a daily basis. The Entellitrak BI will also be configured to automatically generate CVS, 79A, Electronic Questionnaire for Investigation Processing (e-QIP) batch files for processing by OPM and Fingerprints. The integration of Entellitrak BI with these existing OPM data systems will allow D1SB to significantly reduce manual and paper-based processes while increasing the availability of data throughout the investigative lifecycle. This integration will be further expanded by integrating e-QIP data into the Entellitrak BI tool to populate case data as a case is exported to OPM.

The Entellitrak BI application is also set up to deliver an e-Delivery file system in its API environment. Entellitrak BI decrypts the e-Delivery zip, parses the e-Delivery package, and uploads the PDF files to the appropriate Entellitrak BI case files. The Entellitrak application is capable of handling closed cases, stragglers, eFR and REO. Additionally, Entellitrak BI has been configured to translate the available XML data into an Entellitrak BI user interface form for easy viewing by users. Users with the appropriate roles have access to both the translated XML data and uploaded ROI documents. Furthermore, Entellitrak BI solution has been configured for one customer to route cases to certain uses based on case data.

It is an application/system that requires special attention to security due to the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of the information. MicroPact, Inc. of Herndon, VA maintains both hardware and ICATS/Entellitrak software infrastructure to support the GSA Office of Administrative Services (OAS) with maintaining this major application.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
5 C.F.R. parts 2, 5, 731, 732, 736, and 1400, Executive Orders 9397, 10450, 10865, 12333 and 12356, 13478, 13488, 12968, 13467 as amended, 13549, sections 3301, 3302, 7301, and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, and Homeland Security Presidential Directive (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?
GSA/OMA-2

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. [OMB control numbers are assigned to information collections according to the Paperwork Reduction Act. Contact the Regulatory Secretariat Division with questions. That Division prepares, compiles, processes regulatory and general notices for publication in the Federal Register and online.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
GSTARS complies with all GSA retention and disposal procedures in accordance with GSA's NARA-approved records schedules. Record Item Title Retention Instructions Legal Authority Personnel Security Investigative Reports - Personnel Suitability and Eligibility Investigative Reports Temporary. Destroy in accordance with the investigating agency instruction. DAA-GRS-Â2017-0006-Â0022 (GRS 05.6/170) Personnel Security Investigative Reports - Reports and Records created by Agencies Conducting Investigations under Delegated Investigative Authority Temporary. Destroy in accordance with delegated authority agreement or memorandum of understanding. DAA-GRS-Â2017-0006-Â0023 (GRS 05.6/171) Personnel Security and Access Clearance Records - Records of People Not Issued Clearances Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use. DAA-GRS-Â2017-0006-Â0024 (GRS 05.6/180) Personnel Security and Access Clearance Records - Records of People Issued Clearances Temporary. Destroy 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use. DAA-GRS-Â2017-0006-Â0025 (GRS 05.6/181) Index To the Personnel Security Case Files Temporary. Destroy when superseded or obsolete. DAA-GRS-2017-0006-0026 (GRS 05.6/190) Information Security Violations Records Temporary. Destroy 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use. DAA-GRS-Â2017-0006-Â0027 (GRS 05.6/200)

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? Yes

2.1 Explain: If not, please explain.
The SF 85, SF85P, and SF 86 forms completed by applicants prior to background investigations have a Privacy Act Statement, notifying them of the intended usage of information collected and ramifications of not providing the requested information. If notice was provided by a Privacy Act Notice, please describe the content of that notice and/or copy that text here. The information you provide is for the purpose of investigating you for a position, and the information will be protected from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information are governed by the Privacy Act. The agency that requested the investigation and the agency that conducted the investigation have published notices in the Federal Register describing the systems of records in which your records will be maintained. The information you provide on this form, and information collected during an investigation, may be disclosed without your consent by an agency maintaining the

information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses, a list of which are published by the agency in the Federal Register. The office that gave you this form will provide you a copy of its routine uses.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
As part of the investigative process, data is used to conduct preliminary checks in order to grant initial access and start the process of an investigation in order to assess suitability for federal employment and access to sensitive information and to determine if eligible for a security clearance. Information collected and processed in GSTARS is used by agency adjudicators to determine an individual's suitability/fitness for Federal employment and/or a position of trust with the Federal government, and/or for eligibility and access determinations. The information collected about the individual is used to ensure that any person employed by the Federal government is reliable, trustworthy, of good conduct and character, and loyal to the United States. The data collected is relevant and necessary for GSTARS to act as an authoritative data source and to allow the Personnel Security Division to properly adjudicate background investigations for the agency.

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?
GSTARS does not create or aggregate new data about the individual.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
GSTARS has implemented the required security and privacy controls according to NIST SP 800-53. GSTARS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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

3.4 Explain: Please elaborate as needed.
The GSTARS System does not monitor the public, GSA employees, or Contractors.

3.5 What kinds of report(s) can be produced on individuals?
No reports are currently created; however, GSTARS may create reports related to the status of investigations and to maintain accuracy of system records.

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?
GSTARS does not de-identify data for reporting.

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?
Federal Agencies

4.2How: If so, how will GSA share the information?
No. Access to the system will only be granted to employees and contractors of the Personnel Security Division that require access to the information to initiate the paperwork for an investigation and adjudication background investigations on personnel.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Information is collected from the individual using the OF 306, Declaration for Federal Employment, SF 85, 85P and 86 Security Questionnaires, and other federal employment application forms received from OHRM, OPM, DCSA, and FBI as part of the background investigation process.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?
Not at this time. However, GSTARS could share/link with the HRLinks system in the future.

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

4.4NoAgreement: Why is there not a formal agreement in place?
N/A

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
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 information collected about the individual in the course of the investigation is used to ensure that any person employed by the Federal government is reliable, trustworthy, of good conduct and character, and loyal to the United States. Information is collected directly from applicants, employees, volunteers, student interns, visitors, and others who require access to GSA facilities and/or information systems. PII is provided when individuals complete OPM's e-QIP (Electronic Questionnaire for Investigations Processing) as well as the Optional Form (OF) 306, Declaration for Federal Employment. The information collected in the security form is used by Defense Counterintelligence and Security Agency, Office of Personnel Management and Federal Bureau of Investigation investigators to conduct the necessary background investigations. The individual's PII information is verified during pre-employment checks; if incorrect, the individual will be contacted.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Access to the system will be employees and contractors of the Personnel Security Division that require access to the information to initiate the paperwork for an investigation and adjudication background investigations on personnel. This includes Personnel Security and the Security Programs Branch. The Personnel Security Division personnel are, by law, bound by the Privacy Act. Specific information about an individual will be shared with Agency employees who have a "need to know". Access is based on the principle of least privilege that a user requires to perform his or her job duties. Access requests are approved by 2 to 4 levels of approval depending on access requested. The access is granted based on functional needs, and users' access will be restricted by the system. System Administrator's assign appropriate permissions and provide access to the specific data set within the system via Windows Active Directory

group membership. GSTARS classifies users into several 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. Users must meet background investigation and training requirements prior to gaining access to GSTARS.

6.1b: What is the authorization process to gain access?
Users only have access to the data for which they have been granted access to. This is done via groups and roles. These groups and roles are periodically reviewed by the system administrators to ensure a user does not have access to data for which they are not authorized to retrieve or view. Each user role is reviewed once a year during the recertification process.

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.
3/25/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
GSTARS has implemented the required security and privacy controls according to NIST SP 800-53. GSTARS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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?
GSTARS has implemented the required security and privacy controls according to NIST SP 800-53. GSTARS employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
All forms requesting information include a Privacy Act Notice in compliance with the Privacy Act of 1974.

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.
Applicants are given the opportunity to decline to provide their own information by not submitting their information for the employment opportunity. Declining to provide their information simply means that the individual chooses not to participate in the hiring process for the employment opportunity.

7.2: What are the procedures that allow individuals to access their information?

The system is maintained electronically in the Office of Mission Assurance, Personnel Security Division, Personnel Security Branch. Personnel seeking records from GSTARS may file a Privacy Act request. Individuals may contact the Personnel Security Branch via phone, 202 208-4296 or by email gsa.securityoffice@gsa.gov..

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
The individual entering data into the e-QIP system can modify the information to ensure all the fields entered into system is accurate prior to submitting the form. Once the form has been edited and submitted as final copy, the individual cannot modify that information in the 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.
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. 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.

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. 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.