GSA Security Tracking and Adjudication Record System (GSTARS)

Privacy Impact Assessment (PIA)

May 6, 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:

- Urline M Richardson

Signature Page

Signed:

DocuSigned by:
Matthew Regan
92526A8616CB470...
Information System Security Manager (ISSM)

DocuSigned by:
Urline Richardson
A6D272AA74B041D...
Program Manager/System Owner

DocuSigned by:
Richard Speidel
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
4/20/2020	Revised - Comments Addressed	3.1
5/6/2020	PIA Approved	3.2

Table of contents

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 GSTARS. Personnel Security Branch (D1SB) GSA office conducts background investigations (BIs) on GSA applicants and employees (both federal and some contractor) to determine their: 1) initial suitability/fitness for employment with GSA; 2) continued suitability/fitness for employment with GSA and external agencies GSA supports; 3) eligibility to occupy a national security position or access classified information; and 4) eligibility for access to federal facilities and/or information technology systems.

The purpose of this system is to manage the personnel security clearance and investigations program. It will maintain the agency background investigations received from the Office of Personnel Management e-Delivery tool. It will be used to collect and maintain records of processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. To accomplish its mission (D1SB) GSA office must, in the course of maintaining GSTARS, 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]

A. System, Application, or Project Name:

The GSA Security Tracking and Adjudication Record System (GSTARS) is a system that falls under the Enterprise Applications Services (EAS) FISMA system.

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 4000 unique records in GSTARS, and new records are added daily.

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

Full Name • Social Security No. • 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) *is a web-based application used by the Personnel Security Branch as a tool for tracking of applicants and existing employee background investigations associated with job vacancies and employee investigations and reinvestigations. The tracking of individual investigations maintained in GSTARS to manage the movement from initiation to closing of an investigation.* ●

Descriptions of what PII is collected, its maintenance, use, or its dissemination and who or what it is collected from; and,

Information voluntarily provided in the employment submission package from the applicants, employees, interns, volunteers, and others, include the resume, GSA Form 3665, OF Form 306, military personnel record, educational transcripts, and the security questionnaires (SF85, SF85P, SF86). ● *Descriptions of how the system, application, or project collects and uses*

PII, including an example that illustrates what happens to the PII from the time it is collected until it is destroyed.

If applicable, reference any associated system of records notice (SORNs) by Federal Register citation (XX FR XXXX, Date) in the overview. You may later reference associated SORNs by GSA name and number only.]

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 C.F.R. parts 2, 5, 731, 732, 736, and 1400, Executive Orders 9397, 10450, 10865, 12333 and 12356, 13488, 12968, 13467 as amended, 13549, sections 3301 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? If so, what System of Records Notice(s) apply/applies to the information?

Yes, GSA/OMA-2

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.

[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, and processes regulatory and general notices for publication in the Federal Register and online.

No ICR has been submitted.

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.

GSTARS complies with all GSA retention and disposal procedures specified by 1820.1 CIO P GSA Records Maintenance and Disposition System. Records contained in the GSTARS system will be retained consistent with section 5.6 of NARA General Records Schedule, "Personnel Security

Records"; items 170, 171, 180, 190, 200. See https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf.

***Temporary.** Destroy in accordance with the investigating agency instruction.*	*DAA-GRS-2017-0006-0022*
Temporary. Destroy in accordance with delegated authority agreement or memorandum of understanding.	*DAA-GRS-2017-0006-0023*
Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.	*DAA-GRS-2017-0006-0024*
Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.	*DAA-GRS-2017-0006-0025*
Temporary. Destroy when superseded or obsolete.	*DAA-GRS-2017-0006-0026*

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.

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.

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?

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? If so, how will this data be maintained and used?

No, 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?

No.

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

GSTARS does not de-identify data for reporting.

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

GSTARS limits information to only what is required to carry out employment activities.

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?

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 or is it taken from another source? If so, 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, 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? If so, who and how? Is a formal agreement(s) in place?

Not at this time. However, GSTARS could share/link with HRLinks system in the future.

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?

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.

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?

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 of 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.

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's role is reviewed once a year during the re-certification process.

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

Yes, Enterprise Application Services (EAS), which GSTARS fall under ATO was signed 3/26/2020.

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? If so, 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

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.

All forms requesting information include a Privacy Act Notice in compliance with the Privacy Act of 1974. 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 procedures 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? If so, how?

Individuals may contact the Personnel Security Branch via phone, 202 208-4296 or by email gsa.securityoffice@gsa.gov to address concerns.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

GSA has developed, implemented, and regularly updates its IT Security Awareness and Privacy Training as part of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities.

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.

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

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

---

[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.