GSA Security Tracking and Adjudication Record System (GSTARS) Privacy Impact Assessment

Dated: May 7, 2018

Prepared by
Arpan Patel, ISSO
General Services Administration
OCIO - Staff Offices ISSO Support Branch

PART I PIA Contacts and Qualification QUESTIONS
A. Contact Information

Date: March 15, 2018
Minor Application: GSA Security Tracking and Adjudication Record System.
Office of Responsibility: Office of Mission Assurance. Management and oversight for the GSA Security Tracking and Adjudication Record System Minor Application is provided by: General Services Administration (GSA) Office of the Chief Information Officer (OCIO) OCIO Headquarters (HQ) 1800 F Street, NW Washington, DC 20405

B. Qualification Questions

Question	Explanation/Instructions
1. Does your system collect any information in identifiable form (personal data) on the general public? (YES or NO. If YES, a PIA is required).	Yes.
2. Does your system collect any information in identifiable form (personal data/information) on government employees? (YES or NO. If YES, a PIA is required).	Yes.
3. Has a PIA been done before for the system? (YES or NO)	No.

PART II SYSTEM ASSESSMENT
A. Data in the System

Question	Explanation/Instructions
1. Describe all information to be included in the system, including personal data.	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).
1.a. What stage of the life cycle is the system currently in?	Development/Implementation
2.a. What are the sources of the information in the system?	Records are obtained from a variety of sources: information is provided by the applicant in his or her security questionnaire and Office of Human Resources Management submits security packages on applicants to start the investigation process. Records are also obtained from the Office of Personnel Management and National Background Investigations Bureau that conduct background checks using written consent provided by the applicant against public records and government agencies systems such as Internal Revenue Service (IRS) and FBI.
2.b. What GSA files and databases are used?	GSTARS verifies the investigation type, date, and clearances for employees against information in HR Links (CHRIS replacement). GSTARS uses contact information from the Credential and Identity Management System (GCIMS) when required as part of the investigation process. Both systems are used to gather information collected to verify addresses, identities, supervisors, and contact information; etc., for investigative purposes.
2.c. What Federal agencies are providing data for use in the system?	The Office of Personnel Management (OPM), Federal Bureau of Investigation (FBI), and GSA.
2.d. What State and local agencies are providing data for use in the system?	National Crime Information Center (NCIC); Specific authorizations are used when required: for example staff complete GSA Form 3665, Authorization to Obtain Credit Report and Authorization of Release of Information.
2.e. What other third party sources will the data be collected from?	Authorized Personnel Security staff access credit report information from Equifax as part of preliminary checks on applicants and employees assigned to national security positions.
2.f. What information will be collected from the individual whose record is in the system?	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.
3.a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	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 OPM and FBI investigators to conduct the necessary background investigations.
3.b. How will data be checked for completeness?	The individual's PII information is verified during pre-employment checks; if incorrect, the individual will be contacted.

3.c. Is the data current? How do you know?	The information collected will be verified by OPM and OPM investigators to conduct the necessary background investigations.
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	OPM's e-QIP (Electronic Questionnaire for Investigations Processing) as well as the OF 306, Declaration for Federal Employment.

B. Access to the Data

Question	Explanation/Instructions
1. a. Who will have access to the data in the system?	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".
1.b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	HR Links data is exempt from FOIA request under exemption #6 (information involving matters of personal privacy.) In accordance with the Insider Threat Classification guide dated 2013, Insider Threat data analysis and results of inquiries will not be housed in GSTARS. For Insider Threat specific information, contact the Insider Threat Program directly.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	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.
3. Will users have access to all data in the system or will the user's access be restricted? Explain.	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.
4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?	System will not allow access, or the ability to browse, beyond what the user has been approved access for. All individuals (i.e. System Administrators, Database Administrators, Users, Processing Personnel, Supervisors and Managers) granted access to the system are covered by the same rules of behaviors that delineate the responsibility and expectations for all individuals with access to the system, and the consequences of behavior not consistent with the rules. In addition, they must adhere to the standards set forth in the Privacy Act of 1974 when dealing with any data.

	Logical Access, Operational, and Management controls are established to maintain data security. These controls include user account management, system auditing and monitoring, timely removal of terminated employees' system access and the modification of employee's system access when they change job positions and functions. Additionally user permissions are validated annually during user recertification. Security controls for a medium risk system as defined by NIST in its publication SP 800-52 have been implemented in the system.
5.a. Do other systems share data or have access to data in this system? If yes, explain.	Not at this time; but GSTARS could share/link with CHRIS (Comprehensive Human Resources Integrated System) and GCIMS (GSA Credential & Identify Management System) and the new HR Links system (CHRIS replacement) in the future.
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	The Director, Office of Enterprise Solutions, General Services Administration, 1800 F Street, NW., Washington, DC 20405.
6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	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.
6.b. How will the data be used by the agency?	The records in this system will be used for tracking all personnel security information related processes for the individual during his or her tenure with GSA.
6.c. Who is responsible for assuring proper use of the data?	Deputy Director, Personnel Security Branch Phone: (202) 208-4296 E-mail: gsa.securityoffice@gsa.gov Organization Title and Correspondence Code: Personnel Security Branch, (D1SB) All Personnel Security Division personnel are briefed on the use and protection of Privacy Act data as per the GSA training requirements and in house training.
6.d. How will the system ensure that agencies only get the information they are entitled to?	The Director, Office of Enterprise Solutions, as the system owner, will establish accounts and access as to NOT allow access, or the ability to browse, beyond what the user has been approved access for. As discussed above, access requests are approved by 2 to 4 levels of approval depending of access requested and the system only allows users to send reports to other authorized users of the system.
7. What is the life expectancy of the data?	System records are retained and disposed of according to GSA records maintenance and disposition schedules and the requirements of the National Archives and Records Administration.
8. How will the data be disposed of when it is no longer needed?	System records are retained and disposed of according to GSA records maintenance and disposition schedules and the requirements of the National Archives and Records Administration.

C. Attributes of the Data

Question	Explanation/Instructions
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. 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.
2.a. Will the system derive new data or	No

create previously unavailable data about an individual through aggregation from the information collected?	
2.b. Will the new data be placed in the individual's record (client or employee)?	N/A
2.c. Can the system make determinations about individuals that would not be possible without the new data?	N/A
2.d. How will the new data be verified for relevance and accuracy?	N/A
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	N/A
3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	N/A
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Records are retrievable by a combination of first name, last name, and/or social security number. Group records are retrieved through a combination of search parameters (e.g. employee type, employment status, region, etc.) through the GSTARS portal.
5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decision making; and d. Use of new technologies. How are the effects to be mitigated?	There are no identified potential effects on the privacy rights of individuals. Risk is mitigated because no new data is derived from the original data and also existing, proven web technologies are used in building this federal system. Also, GSTARS does not provide decision making capabilities, but only acts as a tracking system and authoritative data source.

D. Maintenance of Administrative Controls

Question	Explanation/Instructions
1.a. Explain how the system and its use will ensure equitable treatment of individuals.	Privacy data is not involved in the decision making processes. The system does not make decisions or suggest courses of action. GSTARS uses standard screens to collect and store individual information according to the requirements of standard forms for background investigations, thereby ensuring equitable treatment.
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	Only personnel with a direct need to either create or use the data in GSTARS are granted access to the system. The most sensitive areas of the system are only made available to personnel with a direct need-to-know in the Personnel Security Division.
1.c. Explain any possibility of disparate treatment of individuals or groups.	The risk of potentially disparate treatment is decreased by the fact that GSTARS does not provide decision making capabilities, but only acts as a tracking system and authoritative data source. In addition, all GSA staff

	are required to complete the mandatory insider threat training: https://insite.gsa.gov/portal/content/697806.
2.a. What are the retention periods of data in this system?	GSA personnel security records relating to individuals are retained and disposed of in accordance with NARA General Records Schedule 5.6, items 010, 170, 171, 180, 181, 190, 200, 210, 220, and 230.
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	The process for destroying GSTARS information is documented in the records schedule referenced above and in accordance with GSA's Records Management Program.
2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The GSA Personnel Security Handbook describes processes to update information in case of employment events for all employees which in turn result in an update of personnel data. Also the Personnel Security Branch plans to periodically verify GSA personnel status through the HR Links system (CHRIS replacement). Additionally, we receive monthly "separation" notices from HRLinks of all departing employees which helps the data in GSTARS to keep up to date.
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)?	No
3.b. How does the use of this technology affect individuals' privacy?	The privacy will not be affected by the technologies. Tracking mechanisms for individual's information are not employed. Information is handled in accordance with GSA's privacy policies and Federal laws.
4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No
4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No
4.c. What controls will be used to prevent unauthorized monitoring?	N/A
5.a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.	GSA Credential & Identity Mgmt System (GCIMS) GSA/CIO-1.
5.b. If the system is being modified, will the SOR require amendment or revision? Explain.	This is a new system that is covered by an existing GSA SORN (see above).