GSA Real Estate Exchange

Privacy Impact Assessment

January 29, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Instructions for GSA employees and contractors:

This template is designed to assist GSA employees and contractors in complying with the E-Government Act of 2002, Section 208, which requires GSA to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The template also accords with 1878.2A CIO P - Conducting Privacy Impact Assessments; is designed to align with GSA businesses 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 demonstrates how GSA ensures that privacy protections are built into technology from the start, not after the fact when they can be far more costly or could affect the viability of performing GSA's work. Completed PIAs are made available to the public at gsa.gov/privacy (https://www.gsa.gov/portal/content/102237).

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. For example:

This document contains important details about *[system, application or project name]*. *[GSA office]* may, in the course of *[program name]*, collect personally identifiable information ("PII") about the people who use such products and services.

An example of a completed PIA is available at:
https://www.gsa.gov/portal/getMediaData?mediaId=167954

If you have any questions, send them to gsa.privacyact@gsa.gov.

Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Revised to include questions about third party services on websites and robotics process automation (RPA).	2.0
6/26/2018	New question added to Section 1 regarding "Information Collection Requests"	2.1

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 GSA Real Estate Exchange (G-Rex). PBS- IT may, in the course of G-REX 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, 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

GSA Real Estate Exchange (G-REX).

System, application or project includes information about

G-REX supports over 2700 users from Central Office (CO) and the GSA's eleven (11) regions. In addition to internal users, G-REX supports shared service provider broker contractors via the PBS Portal Extranet environment.

System, application or project includes

The system includes these data fields:

- Name
- Contact Information (e.g., address, telephone number, email address)
- Social Security Number, Tax Identification Number

The system includes these data categories:

- Financial Information
- User and Online Information

Overview

G-REX is a mission-critical, web-based lease acquisition application. It provides PBS, its delegated agencies, and its national brokers with a task-based workflow to manage the complete life cycle of leasing transactions. G-REX also provides reporting and dashboard tools to support General Accounting Office (GAO) and audit requirements. Using predefined workflows Leasing Specialists, Lease Contract Officers, agencies and brokers with specific delegated authority perform tasks to identify, acquire and manage leased space throughout the Government. The information collected by G-REX users includes milestone dates, lease property details, property requirements, task assignments, and lease policy conformance data. This information is used to assess, evaluate, award and assist the lease users in managing the lease lifecycle.

GSA delegates leasing tasks to other Federal Agencies. G-REX is used to track delegated lease requests and leasing activities to monitor agency compliance with leasing laws, regulation and policy. Where applicable, implementation of the system and its efficiencies provide accountability and increase transparency into leasing activities leading to improved customer satisfaction. G-REX supports PBS leasing activities across the Realty Services Enclave including other National Applications such as RWA Entry and Tracking System (RETA) and Occupancy Agreement (OA) Billing.

G-REX establishes a national leasing procurement process. The application automates daily tasks of realty specialists through document management, electronic templates, communication and intra-application integrations. G-REX includes information about leases, buildings, offerors and lessors.

G-REX may include documents of offeror-submitted material that potentially contains PII in the form of a taxpayer identification number (TIN) or social security number (SSN). G-REX also maintains the offeror/lessor business addresses and telephone number, which might be offeror/lessor home address and telephone number. The offeror/lessor address and telephone number are needed for communication between the realty specialist and the offeror/lessor. The Internal Revenue Service (IRS) requires that a TIN or SSN is submitted with the offer.

The offeror provides the data when submitting a lease offer. Users input and scan information into G-REX. External agency contracting officers provide requirements information through electronic submissions. The G-REX user collects the data directly from the offeror/lessor. This information is entered into G-REX and is only acceptable with required field formats and values. Additionally, PBS’s Delegated Leases Program Team reviews submissions from other Federal Agencies for accuracy.

G-REX users are responsible for maintaining accurate and timely information. As part of the lease checklist regions may review and audit files to ensure accuracy. Additionally, the G-REX data dictionary contains attributes of how the data is stored in the application.

G-REX provides role-based information to the information housed within the system. There are roles that limit access to information based on the user being a GSA employee, embedded contractor working on behalf of G-REX (Broker Contractor) for a specific project, and delegated agency user. Administrative privileges are reserved for GSA employee users.

G-REX user access to data is determined by a request submitted and managed through PBS Portal's User Identity Management System (UIMS), through which the request is processed by designated approvers. The request records are maintained by UIMS. The PBS Portal provides authentication and authorization at user login. G-REX provides security by role, region, and project assignment, therefore, limiting access to only that which a user needs for a specific job.

G-REX has controls in-place to prevent the misuse of data such as tracking changes made to tasks, evaluations, status, and dates. G-REX users cannot delete documents and records. G-REX tracks user's data modifications on critical transactions with audit trails on table, including the history of dates and time changes. Business data is time stamped according to the most recent update.

G-REX receives transactional updates via Cast Iron from the Real Estate across the United States (REXUS) application. The data from REXUS may include project and property information. Nightly updates via extract, transform, load (ETL) scripts update the PBS Business Intelligence (BI) Framework reporting tool. The BI Framework data is used for G-REX reporting. Additionally, G-REX plans to exchange information with Salesforce Workspace Org in the future through: (1) Automated Advanced Acquisition Program (AAAP) (Lease Offer Platform) (LOP) application about offerors that allows the commercial real estate community an opportunity to offer building space for lease to the Federal Government; and (2) Real Estate Tax (RET) Portal to automate submission of tax documents to G-REX document repository.

G-REX project and leasing data are maintained in the database indefinitely. Documents, e-mail correspondence, and communication logs cannot be deleted by users. The G-REX PM is responsible for ensuring the data is handled and disposed of properly. Data is disposed of according to the National Archives and Records Administration (NARA) authority number NC1-121-81-1. Lease cases must be maintained for at least eight (8) years.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA is collecting this information because G-REX supports the General Services Administration's mission for delivering superior workspaces through innovation at the best value. G-REX standardizes a national leasing transaction lifecycle and automates the daily tasks of realty specialists through document management, electronic templates, a workflow engine, communication facilitation, and Public Building Services (PBS) common services integration.

1.2 What legal authority and/or agreements allow GSA to collect the information?

Federal Property and Administrative Service Act as amended (40 U.S.C. Sec.585)

1.3 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 being collected?

GSA SORN PBS-5, "e-Lease"

1.4. Has any 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.

Pending

1.5. 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.

Data is disposed of according to the NARA authority number NC1-121-81-1. Lease cases must be maintained for at least eight (8) years.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

As the system does collect a form of Personally Identifiable Information in the collection of SSNs and TINs, there are privacy risks that relate to the purpose of the collection. G-REX, however, has controls in-place to prevent the misuse of data such as tracking

changes made to tasks, evaluations, status, and dates. G-REX users cannot delete documents or other system records. G-REX tracks user's data modifications on critical transactions with audit trails on table, including the history of dates and time changes. Business data is time stamped according to the most recent update.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Prior notice is given in the eLease SORN and the G-REX Privacy Act Statement, which states:

"GSA is asking for your TIN/SSN data and offeror/lessor address and telephone number in order to perform leasing activities on projects for which PBS has delegated leasing authority to those agencies. The offeror/lessor address and telephone number are needed for communication between the realty specialist and the offeror/lessor. The IRS requires that the TIN is submitted with the offer. This collection of information is authorized by the E-Government Act of 2002 (P.L. 107-347, 44 USC § 3501). GSA may use this information pursuant to its published Privacy Act system of records notice, GSA SORN PBS-5."

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Not applicable as notice is given before the collection of data.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII 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 Whose information is included in the system, application or project?

G-REX includes information about leases, buildings, offerors and lessors.

3.2 What PII will the system, application or project include?

G-REX may include documents of offeror-submitted material that potentially contains PII in the form of a TIN or an SSN. G-REX also maintains the offeror/lessor business addresses and telephone number, which might be the offeror/lessor home address and telephone number.

3.3 Why is the collection and use of the PII necessary to the system, application or project?

G-REX may include documents of offeror-submitted material that potentially contains PII in the form of a TIN or SSN. G-REX also maintains the offeror/lessor business addresses and telephone number, which might be offeror/lessor home address and telephone number. The offeror/lessor address and telephone number are needed for communication between the realty specialist and the offeror/lessor.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

G-REX needs to aggregate data across different tables to be able to provide roll up project data visualizations, such as national and regional project reports. Aggregation of data is also required to produce project-specific dashboards to allow users to manage projects where they are assigned.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

GSA protects personal information in G-REX as described in Section 6, below.

3.6 Will the system monitor the public, GSA employees or contractors?

No, G-REX will not monitor the public, GSA employees or contractors.

3.7 What kinds of report(s) can be produced on individuals?

G-REX provides role-based access to users. Depending on their role, a user may be able to download excel files containing data related to:

- Customer Milestones for Projects
- Disaster Leases in the system

- Broker Evaluations
- Delegations Projects - Approved/ Denied

These files are only accessible to those users with the appropriate level of security access.

3.8 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?

G-REX does not provide users the ability to generate reports on individual users. Depending on their level of access, a user may be able to download one of the reports mentioned above and use excel to manipulate data to produce pivot tables with basic information, e.g. what projects are associated with an individual, etc. However, there is no ready-to-view report available in the system.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

G-REX does not provide users the ability to generate reports on individuals.,

SECTION 4.0 LIMITS ON USES AND SHARING OF 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. Information in G-REX is limited to leases, buildings, offerors and lessors, which allow G-REX to establish a national leasing procurement process.

G-REX may include documents of offeror-submitted material that potentially contains PII in the form of an SSN. G-REX also maintains the offeror/lessor business addresses and telephone number, which might be offeror/lessor home address and telephone number. The offeror/lessor address and telephone number are needed for communication between the realty specialist and the offeror/lessor. The IRS requires that the TIN is submitted with the offer.

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?

Data from the system may be reported to other agencies, OMB and Congress through Business Intelligence (BI) reporting (milestone dates, budget projections, etc) but not G-REX directly. No sensitive information is shared. Users from other federal agencies and broker contractor firms are provided G-REX access but are limited to accessing information pertinent to projects assigned to them. GSA does often provide a copy of the lease to the agency for the space they occupy. That is in the normal course of business.

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)?

Yes, information is collected directly from the individual. The offeror provides the data when submitting a lease offer. Users input and scan information into G-REX. External agency contracting officers provide requirements information through electronic submissions. The G-REX user collects the data directly from the offeror/lessor. This information is entered into G-REX and is only acceptable with required field formats and values. Additionally, PBS's Delegated Leases Program Team reviews submissions from other Federal Agencies for accuracy.

G-REX users are responsible for maintaining accurate and timely information. As part of the lease checklist regions may review and audit files to ensure accuracy. Additionally, The G-REX data dictionary contains attributes of how the data is stored in the application.

G-REX receives transactional updates via Cast Iron from the REXUS application. The data from REXUS may include project and property information.

G-REX does not use information from commercial sources or publicly available data.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

G-REX receives transactional updates via Cast Iron from the REXUS application. The data from REXUS may include project and property information. Nightly updates via extract, transform, load (ETL) scripts update the PBS BI Framework reporting tool. The

BI Framework data is used for G-REX reporting. Additionally, G-REX plans to exchanges information with Salesforce Workspace Org in the future through: (1) Lease Offer Platform (LOP) that allows commercial real estate community an opportunity to offer building space for lease to the Federal Government; and (2) Real Estate Tax (RET) Portal to automate submission of tax documents to G-REX document repository.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

As discussed above, other agencies, OMB and Congress may access certain non-sensitive leasing information through Business Intelligence (BI) reporting (milestone dates, budget projections, etc.) but cannot access G-REX directly.

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 be verified for accuracy and completeness?

The offeror provides the data when submitting a lease offer. Users input and scan information into G-REX. External agency contracting officers provide requirements information through electronic submissions. The G-REX user collects the data directly from the offeror/lessor. This information is entered into G-REX and is only acceptable with required field formats and values. Additionally, PBS's Delegated Leases Program Team reviews submissions from other Federal Agencies for accuracy.

G-REX users are responsible for maintaining accurate and timely information. As part of the lease checklist regions may review and audit files to ensure accuracy. Additionally, The G-REX data dictionary contains attributes of how the data is stored in the application.

G-REX user access to data is determined by a request submitted and managed through GSA IT Enterprise Document Management System (EDMS) Alfresco, through which the request is processed by designated approvers. The request records are maintained by UIMS. EDMS Alfresco provides authentication and authorization at user login. G-REX provides security by role, region, and project assignment, therefore, limiting access to only that which a user needs for a specific job.

G-REX has controls in-place to prevent the misuse of data such as tracking changes made to tasks, evaluations, status, and dates. G-REX users cannot delete document and records. G-REX tracks user's data modifications on critical transactions with audit trails on table, including the history of dates and time changes. Business data is time stamped according to the most recent update.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

G-REX user access to data is determined by a request submitted and managed through EDMS Alfresco, through which the request is processed by designated approvers. The request records are maintained by UIMS. EDMS Alfresco provides authentication and authorization at user login. G-REX provides security by role, region, and project assignment, therefore, limiting access to only that which a user needs for a specific job.

Access to G-REX does not necessarily translate into access to projects within G-REX (unless your role permits). The G-REX user is assigned role(s) based on their job function. The user needs to be provided access to specific projects to be able to work them in the capacity of roles assigned to them.

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?

All users have their employee status categorized with a sensitivity level in accordance with the Position Risk Description security control (PS-2) from National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 4. Employees (or contractors) of GSA are considered Internal Users or Organization Users. All other users are considered external users or Non-Organization Users.

G-REX user accounts are requested and approved within UIMS. Organization users (Internal) of G-REX consist of GSA employees and contractors. Non-organization users consist of external Federal Agency personnel. Account provisioning is handled through G-REX and the GSA's Enterprise Internal Active Directory. A user's privileges are based on their group/role. G-REX provides the ability to create business rules, based on agency policies and associated regulations, to implement business user groups/role incompatibility and identify combinatory role(s) with conflict of interest.

Organization Users: Organization users in G-REX must participate in the annual recertification process. If a user's recertification is rejected, their access within SecureAuth/OpenDJ is removed and then synced to the G-REX application. G-REX also uses the UIMS ninety (90) day inactivity deactivation process to remove access of users that have not logged into the application in ninety (90) days.

Non-Organization Users: Extranet users in G-REX are given a twelve (12) month expiration date when the Extranet PBS Portal account is created. At the beginning of the month (based on expiration date) the PBS National Help Desk sends an e-mail to the extranet users requesting information regarding their need to continue to have access to the extranet PBS Portal. If the user provides a response to the e-mail with the explanation of why there is still a need, the request is sent to the PBS Business Line and the PBS Portal PM for approval and the expiration is reset for another twelve (12) months. If the users states access is no longer needed or does not respond, the account is disabled. This is a manual recertification process that proceeds throughout the year based on the original assigned expiration date.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes. The G-REX Authority to Operate (ATO) is dated August 17, 2016 and has been signed by the AO and CISO. The G-REX authorization is updated every three (3) years or there is a major system change. The current G-REX ATO expires August 17, 2019.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

G-REX has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ variety of security measures defined in the System Security Plan (SSP) 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, along with system and information integrity.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

The system owner and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer, along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

G-REX has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ variety of security measures defined in the System Security Plan (SSP) 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, along with system and information integrity.

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 are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

G-REX users are provided a Privacy Act Statement and can review the eLease SORN to understand how the information will be retrieved and used by GSA. Lessors may request a TIN from the IRS instead of providing an SSN and have other options that may decrease the sensitivity of the information they must provide while using G-REX.

7.2 What procedures allow individuals to access their information?

Users are allowed to keep the information they provide via G-REX up-to-date.

7.3 Can individuals amend information about themselves? If so, how?

Yes, users can keep the information they provide via G-REX up-to-date.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

GSA mitigates the potential privacy risks related to participation by providing users with notice and allowing them to keep the information they provide via G-REX up-to-date.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

The GSA Information Technology (IT) Security Policy CIO P 2100.1 requires GSA associates and contractor personnel to complete security and privacy awareness training annually. New and returning GSA employees and contractors must complete the basic security awareness training and privacy training within thirty (30) days of employment.

- The training is administered through GSA OLU. This training requires electronic acknowledgement when the employee has completed the course.
- Per the GSA Information Technology (IT) Security Policy CIO P 2100.1, if an employee or contractor does not complete the training during the thirty (30) day training period, their GSA e-mail access is immediately terminated.

The G-REX PM coordinates with users and contractor personnel to ensure that all users complete the annual online IT security training course entitled, Protecting GSA's IT Resources, as required by GSA.

G-REX external delegated users comply with their agency policies.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

As discussed above, GSA requires employees, associates and contractor personnel to complete security and privacy awareness 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, application or project ensure that the information is used in accordance with the stated practices in this PIA?

G-REX relies on the common controls provided by TechOps, the infrastructure operations group that supports PB-ITS applications, to implement the GSA settings for the servers on which the application resides.

TechOps has access to the servers and networking equipment and is responsible for performing operating system level maintenance on the servers.

G-REX relies on Portal and UIMS logging for access control and authentication to the application. The G-REX Appian server further records audit information, including login events, into several log files on disc. This can be used for logon traceability for access from mobile devices (G-REX can only be accessed through mobile devices on the GSA network). The G-REX Business Process Management (BPM) engine logs application errors and all user transactions. All data deletions, data access and data changes are logged by the database.

Operating System (OS) level audit logs in the TechOps network are collected and archived within the Security Information and Event Management (SIEM) tool. For additional information on the GSA Enterprise Logging and Auditing, refer to the GSA Logging and Audit Compliance Guidance.

The G-REX Team receives daily application level audit logs from Appian including login auditing to G-REX (timestamp, username, and if the login was successful or failed) and server level auditing. Appian protects audit authorization access to management audit functionality to only Appian Administrators.

GSA conducts a security assessment every three (3) years or when a major change occurs for G-REX. In addition, annual FISMA self-assessments are performed to determine the extent to which the security controls are implemented correctly.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

G-REX has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ variety of security measures defined in the System Security Plan (SSP) 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, along with system and information integrity.

---

[1] OMB Memorandum *Preparing for and Responding to a 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.