NBC Studley

Privacy Impact Assessment

March 5, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

richard.speidel@gsa.gov

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 NBC Studley system. Center for Broker Services may, in the course of administering brokerage contracts, 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.

Signature Page

Signed:

_____

Information System Security Manager (ISSM)

_____

Program Manager/System Owner

_____

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for evaluating the PIAs for completeness of privacy related information.

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
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
3/5/2019	Updated Section 6 to be in line with new Azure environment.	2.3

Table of contents

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?

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 NBC Studley. PRAA may, in the course of the GSA Leasing Support Services Contract, 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

NBC Studley

System, application or project includes information about

Contractors and offerors.

System, application or project includes -

Administrative data that may be personally identifiable information during the request for offers phase during a project. The information described below in voluntarily submitted by offerors who intend to do business with the government. This information is only provided when business information is not available:

- Name of the offeror is required for identification and payment purposes.

- Contact Information (e.g., address, telephone number, email address) is required for identification and payment purposes.

- Social Security Number, Taxpayer Identification Number (TIN) or other government-issued identifiers are required for identification and payment purposes.

- Financial Information (bank account information) is required if financial capability to perform is required.

- Information about offerors provided by third parties (e.g. credit reports) is required if financial capability to perform is implicated. In addition, potential lessors are crossed referenced against the debarred bidders list.

Overview

The NBC Studley system, funded, owned and operated by Savills Studley, Inc., is a server housing data related to real estate transactions conducted on behalf of GSA's Center for Broker Services. Savills Studley, Inc. provides real estate services and exchanges data via email and GSA extranet connection to G-REX. Savills Studley brokers may collect information via facsimile, e-mail or hard copy, to form leasing packages on behalf of GSA. Within those packages there are data requirements for offerors seeking to lease space to the government. This typically includes: Name, Lessor Address, Phone Number, Email Address, Tax ID (if not a business this is their SSN) and Financial Account Information (bank account information). This information is uploaded to the government's official data system where it remains until the acquisition project concludes.

Limited PII is collected for the identification of and payment to offerors and lessors for real estate transactions. Access to the file share is limited to personnel authorized to work with GSA data and Savills Studley personnel receive annual training on privacy, data sharing and sensitive information as required by GSA. GSA data is only housed on a secured file share on a server in each of the regional offices. This is the accreditation boundary for the Studley contracts with GSA.

Savills Studley personnel assigned to work on the GSA data use Microsoft Office tools to update the data and save their updates to the document to the GSA file share. The file and print servers are used to provide general file storage and printing services to each respective regional office. Administrative access to the file and print servers are restricted to authorized IT personnel. File and print servers are administered using standard Microsoft tools (Active Directory group membership).

This system leverages the eLEASE SORN which is GSA/PBS-5 document number 73 FR 22414, dated April 25, 2008.

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 maintains information required throughout the lifecycle of a PBS building lease including information about leases, offerors, and lessors. In addition to business contact and identification information (address, telephone number, and Taxpayer Identification Number (TIN)), the system includes personal information on individuals who use personal contact and identification information (home address, telephone, e-mail, and fax numbers, and Social Security Number) for business purposes as sole proprietors. The authority to maintain such the information comes from the Federal Property and Administrative Services Act, as amended (40 U.S.C. Sec. 585). The purpose is to establish and maintain a system for operating, controlling, and managing the Federal property leasing program; tracking leasing projects and workflow activities; and managing associated documents.

System information may be accessed and used by authorized GSA employees and contractors to conduct official duties associated with Federal government building leases. Information from this system may be disclosed as a routine use as described in the eLEASE SORN, but as a general matter, the information collected from potential lessors is only staged for upload.

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

The GSA is the legal authority approving the collection of SSNs by G-REX, via The NBC Studley system: Title 40 of the United States Code, Section 585, authorizes GSA to enter space leases on behalf of Federal agencies for terms up to 20 years.

Offerors/Lessors are required to disclose a taxpayer ID and banking information to complete Representations and Certifications for the Acquisition of Leasehold Interests in Real Property. Personally, Identifiable information may be collected in compliance of the following standard General Clauses:
552.270-30 Prompt Payment - PII may be required to ensure appropriate invoicing and payment in lieu of business data.
52.23223 Assignment of Claims - PII may be required to provide an avenue for pursuit of compensation due in lieu of business data.
52.232.33 System for Award Management - PII may be required to process federal contract awards in lieu of business data.

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?

No, information is not retrieved by a personal identifier. It is retrieved via project identifier (for example contract number or project number). This system leverages the eLEASE SORN which is GSA/PBS-5 document number 73 FR 22414, dated April 25, 2008. This SORN also covers the GSA G-REX System.

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.

Standard and Supplementary forms used in requesting data can be found in *Appendix C: Templates, Forms and Other Guidance*. None of of these require an ICR approved by the OMB.

Documentation provided by offerors to the brokers is submitted on standard forms as outlined in the publicly available PBS Leasing Desk Guide (LDG).

During the Request for Offers or Proposals phase, receipt of offeror packages is acknowledged and offerors are also notified of deficiencies (errors or omissions) within required document packages.

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.

The NBC Studley system does not have a records retention schedule as final documents and records are uploaded into GREX. Project records are maintained in electronic project folders until the project is closed out after occupancy. Prior to closeout by the Government, the Broker confirms that all records have been transferred. Any documentation that is not provided by an offeror, but not specifically requested is uploaded into G-REX as supplemental documentation.

Disposition of GREX records will be according to the National Archives and Records Administration (NARA) guidelines, set forth in the GSA Records Maintenance and Disposition System (OAD P 1820.2A) handbook.

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

There are risks that the provided privacy data could be misused by the agents collecting the data. Additionally, data that has been provided for a lease could be shared externally. To mitigate against these risks, Brokers receive annual training and are required to follow the GSA Standards of conduct. Project data is also restricted to the approved members of the project tems. In the event of a Freedom of Information Act (FOIA) inquiry, all privacy data associated with a project would be redacted/removed prior to responding to the request.

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.

Offerors given the option to provide personally identifiable data in response to an opportunity to lease real property to the government. All privacy data collected for the NBC Studley system is part of a GSA assigned leasing task and is used within the lease request for GSA for the purposes of payment and tax assessment. Offerors may request a

TIN from the Internal Revenue Service, or if unwilling to provide the required information, may decline to offer to lease their property to GSA.

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

No risk has been determined as GSA has not authorized sharing of the data collected to third parties and no information is shared outside of GSA managed systems.

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?

Lessors' seeking to do business with the government, have information included in the NBC Studley system.

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

The NBC Studley system will include the following types of PII:

- Contact Information
- Business Information
- Financial Information
- Social Security Numbers

The Studley broker agents collects information to form leasing packages for the GSA acting as agents of GSA. Within those packages there are the following data requirements which if the lessor would need to provide when enacting a lease with GSA through the Studley brokers. The following information is required if business information is not available:

Lessor Name, Lessor Address, Lessor Phone Number, Lessor Email Address (business or personal as applicable), Lessor Tax ID (if not a business this is their SSN), Financial Account Information (bank account information).

The brokers collect the information within the lease packages and then submit that information manually into the GSA GREX application which is the official repository for this data for GSA. Their access is available through the PBS Extranet Portal. Savills Studley brokers have access to all system resources available to GSA employees including, but not limited to the Google Suite of applications. The broker leverages the GSA Google Drive to store working copies of this data while they are updating it.

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

Offerors/Lessors are required to disclose their a taxpayer ID and banking information to complete Representations and Certifications for the Acquisition of Leasehold Interests in Real Property. Personally Identifiable information may be collected in compliance of the following standard General Clauses:

552.270-30 Prompt Payment
52.23223 Assignment of Claims
52.232.33 System for Award Management

SSNs are only collected when non-PII information, taxpayer IDs, are not available that would satisfy the government's needs.

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?

They system will not create or aggregate new data about the individual.

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

GSA requires reporting on the NBC Studley system for the assessment of information and systems for compliance and operational risk. GSA requires background checks on all personnel with access to the system; initial and follow-on privacy and security awareness training for each individual with access to the system and system managers ensure that antivirus and intrusion detection software scans are completed. Additionally, technical access controls and secure channels for submitting information are managed.

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

No, the system will not monitor the public, GSA employees or contractors.

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

The NBC Studley system is a temporary data repository. No reporting capabilities exist or are planned.

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?

The system does not create reports. The brokers collect the information within the lease packages and then submit that information manually into G-REX.

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

Privacy risks related to data minimization are mitigated by the fact that an offeror can coordinate changes through the appropriate brokerage contact in the Pre-Award phase. Post-Award, the lessor may coordinate with GSA National Office of Leasing to update the information.

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. Collecting PII (SSNs and or financial data) is necessary to ensure appropriate invoicing and payment, to provide an avenue for pursuit of compensation in the event of a claim and to process federal contract awards in lieu of business data.

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?

Information is not shared outside of GSA.

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 provided directly by the offeror.

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?

Information in the NBC Studley system are not directly integrated with any GSA system. However, manual data transfers to G-REX are executed between qualified personnel via GSA's secured network.

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?

The collection of PII is an irregular occurrence. To the extent that it is collected, there may be a risk of unauthorized use. To mitigate this risk, the collection of and access to data is restricted only to those with the appropriate clearance and access need. This is accomplished by limiting personnel access using technical access controls and provision of appropriate privacy and security training.

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?

Once the offeror provides their information, they can coordinate changes through the appropriate brokerage contact in the Pre-Award phase. Post-Award, the lessor would need to coordinate with GSA National Office of Leasing to update the information as it is no longer within the NBC Studley system.

In accordance with Contract Section C.4.3.8 Post Award Services, After Post Occupancy Deliverables have been received, but no later than 60 calendar days after occupancy, the Contractor shall submit the complete Lease file with original documentation to the COR for final approval and acceptance. The Contractor shall complete the Lease file in

accordance with the regional standards unless directed by the National Program Manager. The Lease file documents are to be tabbed in accordance with the GSA National Office Lease File.

There is a checklist for the relevant lease model and setup in the folders/format specified by the Region who placed the task order. Filing conventions may vary by Region. The Contractor shall obtain a certification of receipt from the COR upon file delivery.

Upon submission of the completed Lease file to the COR, the Contractor shall notify the ZCO/OO of the action and that the task order is ready for close-out. The Contractor shall submit via electronic certification to the ZCO/OO that all documents have been scanned or uploaded into G-REX or other systems.

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?

There are no known risks to data quality and integrity. Offerors and lessors are provided an opportunity to correct any errors or omissions during the submission process.

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 data in the NBC Studley system is restricted to:

Broker Program Managers, Broker Transaction Managers, and IT Security Administrators and Transaction assistants who have received GSA security clearances and trainings.

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

GSA has completed an SSP for this application, the current SSP covers the Studley Azure Environment. The Studley Azure Environment has undergone an accreditation and authorization (A&A).

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

The Studley Azure Environment is protected through the infrastructure protections in place by the Studley Azure Government Cloud. This is covered under the Azure Government Cloud FedRAMP assessment and inherited by the Studley system. From a technical perspective protections in place include: To access the environment authorized Studley employees must have a valid Active Directory account within the Studley Azure Government Cloud and a corresponding multifactor authentication token using Azure MFA to gain access to the environment. All work on GSA data is done within the Studley Azure Government Cloud environment, email is conducted leveraging GSA's Google Gmail. File server data is protected by ACLs which allows specific users to access specific file folders depending on their security groups assigned. External access is protected leveraging a Palo Alto Firewall which screens all inbound access requests. The Firewall is configured to only allow requests from the Savills Studley Corporate Network. All other requests are rejected and access will not be provisioned. From a managerial perspective: GSA implements controls relevant to third party vendors and services according to the risks identified to include completion of Risk Assessments. Users of the environment are only authorized by GSA managers and they are required to undergo background investigations prior to access being granted.

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

Users of the NBC Studley system are responsible for reporting and potential incidents directly to the relevant information systems security officer. The officer escalates, reports and responds via approved procedures.

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?

The risk for this system would be if a Savills Studley user is added to the environment without undergoing the GSA required onboarding and approval. Processes are in place with Savills Studley at a contractual level which requires that all access be granted

through the approval of GSA to this environment. Additionally, all approved users through this process are required to take GSA annual privacy and security training that govern the appropriate handling of PII.

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.

Individuals can request a TIN or incorporate in ways which may not require the release of PII to GSA.

7.2 What procedures allow individuals to access their information?

Access to an individual's information is allowed via an individual's FOIA inquiry or Privacy Act request addressed to GSA.

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

No, offerors are not able to directly amend information about themselves, but may follow procedures outlined in section 5.1 to correct errors or omissions.

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?

Risks associated with individual participation are mitigated by the fact that individuals may access their information via a FOIA inquiry or Privacy Act request addressed to GSA.

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.

GSA requires NBC Studley system users to take annual privacy and security training that govern the appropriate handling of PII leveraging access to the GSA Online University (OLU):

- IT Security Awareness and Privacy 101
- Sharing in a Collaborative Environment
- Document Security for Sensitive But Unclassified (SBU) Building Information.

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?

To mitigate potential risks, GSA requires NBC Studly system users to take annual privacy and security training that govern the appropriate handling of PII. System users receive notifications of required training and completion of training is recorded.

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?

GSA utilizes Contracting Officer's Representatives to collaborate with and monitor NBC Studley system compliance as it relates to training and maintenance of clearances. GSA CORs perform quarterly reviews to ensure these mitigation steps are followed.

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?

The NBC Studley system clearly identifies personnel with the capacity to effectively manage and secure data for accountability and auditing. Training is provided to mitigate against potential risks. Additionally, the Contractor is required to participate in required assessments to evaluate the effectiveness of their system.

[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.