



# NBC Studley

## *Privacy Impact Assessment (PIA)*

March 19, 2020

POINT *of* CONTACT

Richard Speidel

[gsa.privacyact@gsa.gov](mailto: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](https://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](mailto:gsa.privacyact@gsa.gov).**

## Stakeholders

Name of Information System Security Manager (ISSM):

- Jonathan Wallick

Name of Program Manager/System Owner:

- Kameshia L. Freeman

## Signature Page

Signed:

DocuSigned by:  
*Jonathan Wallick*  
51A2B47647C34D9...  
Information System Security Manager (ISSM)

DocuSigned by:  
*Kameshia L. Freeman*  
2FD4D56F40AE450...  
Program Manager/System Owner

DocuSigned by:  
*Richard Spidel*  
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
2/20/2020	Removed email field from signature page	3.1

# Table of contents

## SECTION 1.0 PURPOSE OF COLLECTION

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 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.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

## SECTION 2.0 OPENNESS AND TRANSPARENCY

- 2.1 Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

## SECTION 3.0 DATA MINIMIZATION

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

## SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

- 4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection, maintenance, use, or dissemination?
- 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 GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

## **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 *NBC Studley*. To accomplish its mission *the Savills Inc.* must, in the course of executing *national brokerage programs*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information<sup>[1]</sup> 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.<sup>[2]</sup>

### **A. System, Application, or Project Name:**

*NBC Studley*

### **B. System, application, or project includes information about:**

*Contractors and Offerors.*

### **C. For the categories listed above, how many records are there for each?**

*There are over 2100 (NBC 820, NBC2 920, GLS 395) project records that may contain PII for Contractors and/or Offerors.*

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

*Administrative data that may be personally identifiable information during the request for offers phase during a project. The information described below is 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 Numbers (SSN) or Tax Identification Numbers (TIN) or other government-issued identifiers are required for identification and payment purposes.*

*Financial Information, bank routing and tax identification number (TIN) may be required if financial capability to perform is required.*

*Information about individuals provided by third parties (e.g. credit reports, background investigation may be required if financial capability to perform is required.*

## **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 FR22414, dated April 25, 2008.*

## **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?**

*The GSA's the legal authority for collecting SSNs by G-REX, via The NBC Studley system, is: Title 40 of the United States Code, Section 585. That 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.*

**1.2 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?**

*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,*

**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.**

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

**1.4 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.**

*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.*

## **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.**

*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.*

## **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?**

*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.*

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

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

### **3.3 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.*

### **3.4 Will the system monitor the public, GSA employees, or contractors?**

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

### **3.5 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.*

### **3.6 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?**

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

## **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. 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 and how? Is a formal agreement(s) in place?**

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

**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?**

*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.*

**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 will have access to the data in the system. To gain access they are required to apply for and receive GSA security clearances and complete all mandatory training to maintain access. When access is terminated, the access is revoked by contacting HSPD-12 and the IT Service Desk for removal upon notification.*

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

*A three year ATO for the Studley Azure Government Cloud system was issued February 11, 2019. This ATO will expire on 2/12/2022.*

**6.3 How will the system or application be secured from a physical, technical, 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 and respond to 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.*

### **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.**

*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.*

### **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.*

## 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 according to 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.*

---

<sup>[1]</sup>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."

<sup>[2]</sup> Privacy Act of 1974, 5 U.S.C. § 552a, as amended.