U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: USGS Store and IBiS: Print Contract with Rise Business Services, LLC

Date: August 10, 2017

Bureau/Office: U.S. Geological Survey/Enterprise Information

Bureau/Office Contact Title: Supervisory Information Management Specialist

Point of Contact
Email: shpeterson@usgs.gov
First Name: Sibert
M.I.: H
Last Name: Peterson
Phone: (303) 202-4083
Address Line 1: P.O. Box 25286
Address Line 2: Mail Stop 306
City: Denver
State/Territory: Colorado
Zip: 80225

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers

☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The U.S. Geological Survey (USGS) Store sells maps and science publications from the USGS as well as other Federal partners. It is managed by the Science Information Delivery (SID) branch of the USGS Office of Enterprise Information. The USGS is in the process of awarding a print contract though the U.S. Government Publishing Office (GPO) to a new third-party printer, Rise Business Services, LLC. The information collected by the third-party printer is used to fulfill orders for maps and science publications sold by the USGS Store. The intention of the contract is to replace the current USGS in-house facilities for production and fulfillment of map and publication orders.

C. What is the legal authority?

- Earth Science Information Customer Records – Interior, GS-15: Executive Order 3206, as amended; Establishing the Board of Surveys and Maps; OMB Circular A-16, Coordination of Geographic Information and Related Spatial Data Activities; 31 U.S.C. 3512, Executive Order 12906, Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure

- Contract Files – Interior, GS-5: 40 U.S.C. 481, Procurement, Warehousing, and Related Activities

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☒ Other: *Describe* Re-competition of GPO Contract 1815-S

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP)*

010-000000998, 010-000001038, 010-000001012, 010-000001023, 010-000001035 System Security Plan for Enterprise Information

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

- Earth Science Information Customer Records – Interior, GS-15
- Contract Files – Interior, GS-5

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☐ Citizenship
☐ Gender
☐ Birth Date
☐ Group Affiliation
☐ Marital Status
☐ Biometrics
☐ Other Names Used
☐ Truncated SSN
☐ Legal Status
☐ Place of Birth
☐ Religious Preference
☐ Security Clearance
☐ Spouse Information
☐ Financial Information
☐ Medical Information

- ☐ Disability Information
- ☐ Credit Card Number
- ☐ Law Enforcement
- ☐ Education Information
- ☐ Emergency Contact
- ☐ Driver's License
- ☐ Race/Ethnicity
- ☐ Social Security Number (SSN)
- ☐ Personal Cell Telephone Number
- ☐ Other: *Specify the PII collected.*
- ☐ Tribal or Other ID Number
- ☐ Personal Email Address
- ☐ Mother's Maiden Name
- ☐ Home Telephone Number
- ☐ Child or Dependent Information
- ☐ Employment Information
- ☐ Military Status/Service
- ☒ Mailing/Home Address

B. What is the source for the PII collected? Indicate all that apply.

- ☒ Individual
- ☒ Federal agency
- ☐ Tribal agency
- ☐ Local agency
- ☐ DOI records
- ☐ Third party source
- ☐ State agency
- ☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

- ☐ Paper Format
- ☐ Email
- ☐ Face-to-Face Contact
- ☐ Web site
- ☐ Fax
- ☐ Telephone Interview
- ☐ Information Shared Between Systems
- ☒ Other: *Describe* The personally identifiable information (PII) is transmitted from the USGS to Rise Business Services via secure FTP (FTPS).

D. What is the intended use of the PII collected?

It is expected that the PII will be name and address, all for the sole purpose of establishing a shipping destination.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

- ☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The USGS tracks each customer order sent to Rise Business Services through the Integrated Business Solutions (IBiS) system.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

☐ Contractor: *Describe the contractor and how the data will be used.*

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Name and address are sent to Rise Business Services along with order information so that the third-party printer can ship the produced map or publication to the customer.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

All requested PII is optional; however, if the customer declines to provide the information, the USGS will be unable to ship the product to the customer.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☐ Privacy Notice: *Describe each applicable format.*

☒ Other: *Describe each applicable format.*

As part of the GPO 1815-S contract, Rise Business Services was required to submit a PII control plan.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Only the customer name and address are sent to Rise Business Services via FTPS. The USGS tracks customer orders through IBiS. IBiS uses a unique customer number to identify a customer master record, which contains the address, billing information, and product and financial data related to orders in the system. The main identifier for a customer in IBiS is the customer number. A customer can also be identified within IBiS by last name/first name, address attributes, phone number, the last four digits of the credit card number, a purchase order number, and by company name.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*

☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data will only be collected from the customer. An employee or contract employee of SID will review the information at the time it is received in order to verify the accuracy.

B. How will data be checked for completeness?

An employee or contract employee of SID will review the information at the time it is received in order to verify the completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

An employee or contract employee of SID will review the information at the time it is received in order to verify that the data is as current as possible.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

As specified in their PII control plan, Rise Business Services deletes customer information once the order is fulfilled. This retention period is in line with the USGS General Records Disposition Schedule (GRDS) 103-01a, Temporary Issuances, which applies to issuances related to routine administrative functions (e.g., payroll, procurement, personnel property, vehicles, budget, forms, reports, mail, and printing). The disposition schedule for GRDS 103-01a is when the issuance is superseded, canceled, or no longer needed for reference.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Rise Business Services deletes customer information once the order is fulfilled. The destruction process includes: 1) the deletion of ordering and transmission emails upon completion of the order (shipped and received by the customer) and 2) the shredding of label information in shredding bins to coincide with when the emails are deleted.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is minimal impact to privacy as only name and address are transmitted to the third-party printer. The expected lifecycle of the PII related to the GPO 1815-S contract is expected to be dense from initial receipt to deletion/destruction starting with the orders that Rise Business Services is authorized to fulfill. This provision is important because the information will be limited to an electronic email, temporary data storage, shipping label receipt, and the software used to create the label. The process starts with the initial order email and, in a separate transaction, the transmission of the data. The files will be transmitted using Rise Business Services' secure FTP, where the data is downloaded to a production file on their network. The data files will be deleted from the FTP site upon proper download. Only those technicians and staff given credentials to access the production network will have access to the downloaded files, thereby compartmentalizing exposure. The principle of least privilege also leaves an audit trail of employee use and access, allowing Rise Business Services to monitor system misuse. As is normal process at Rise Business Services, each technician and staff access password-protected work stations whose passwords change every 90 days.

Further, the PII content will be located on Rise Business Services' premises in their data center and on their client server, which is completely isolated and separate from the operations and work area. Rise Business Services' network design includes advanced firewalls, and their

architecture is such that they can completely isolate production data from other areas of the operation. In addition, there is no outside physical or electronic access to the network environment, and only employees and management can gain entry. Finally, Rise Business Services systematically employs antivirus software and other web browser cleansing software on its hardware to eliminate virus intrusion.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes *Explanation* Rise Business Services is only sent the customer name and address along with the map or publication order as these are the only information required to fulfill the order.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable; the third-party printer does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Rise Business Services expects to limit use of the software (its internal tracking system and label software) required to perform the orders to only those technicians and staff authorized to know about the orders. This way, the third-party printer reduces the number of people exposed to the information to only those whose official duty it is to fulfill the orders.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Yes, Privacy Act contract clauses were included in the contract. All contractors signed a non-disclosure agreement upon employment. Since this contract provides for the design, development, or operation of a system of records on individuals, the contractor and its employees are considered employees of the agency for the purpose of issuing criminal penalties under the Privacy Act.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*

☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The third-party printer uses audit logs to monitor who accesses customer order information.

M. What controls will be used to prevent unauthorized monitoring?

Rise Business Services has provided training to its staff and to the lead technician to identify PII and the different levels of sensitivity. It is employing a PII control plan to protect the data and to properly dispose of it at the conclusion of the data's lifecycle.

Based upon the project management plan, Rise Business Services expects to limit use of the software (its internal tracking system and label software) required to perform the orders to only those technicians and staff authorized to know about the orders. This way, the third-party printer reduces the number of people exposed to the information to only those whose official duty it is to fulfill the orders. Through the use of their tracking and label creation tools, there is limited exposure of PII, and in the case of creating a label, the PII is erased from the software template once it is printed.

Based upon a precedence of past projects and workflows, Rise Business Services will employ several other safeguards to eliminate the risk of a PII breach including: 1) the deletion of ordering and transmission emails upon completion of the order (shipped and received by the customer), 2) the placing of hard copy work orders containing label information in a locked file cabinet while the order is in production and delivery, 3) the shredding of the label information in their shredding bins to coincide with when the emails are deleted, and finally, 4) the use of other discreet descriptive information in their internal tracking system and subsequently, all reports, to describe an order. Unless a better approach is uncovered, Rise Business Services would use a last name and the numbers of an address to tie a customer to an order, Smith_750, for example.

Rise Business Services views any incident as loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized personnel, have access to or potential access to PII. With this in mind, Rise Business Services' staff and authorized technicians on this program must report any incident, whether suspected or confirmed, to their supervisor immediately. A report is documented with any record of information and actions relevant to the incident. Any alleged violations that may constitute criminal misconduct are escalated to the company's ownership as part of the reporting process.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- ☐ Security Guards
- ☒ Key Guards
- ☒ Locked File Cabinets
- ☒ Secured Facility
- ☐ Closed Circuit Television
- ☐ Cipher Locks
- ☒ Identification Badges
- ☐ Safes
- ☐ Combination Locks
- ☒ Locked Offices
- ☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

- ☒ Password
- ☒ Firewall
- ☒ Encryption
- ☒ User Identification
- ☐ Biometrics
- ☒ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)
- ☐ Public Key Infrastructure (PKI) Certificates
- ☐ Personal Identity Verification (PIV) Card
- ☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- ☐ Periodic Security Audits
- ☐ Backups Secured Off-site
- ☐ Rules of Behavior

☒ Role-Based Training
☐ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☐ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The SID Chief is the Information System Owner and is responsible for oversight and management of the Rise Business Services contract security and privacy controls. The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for any data sent to the third-party printer. The System Manager is responsible for protecting the privacy rights of the public for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the USGS Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The SID Chief is the Information System Owner and is responsible for oversight and management of the Rise Business Services contract security and privacy controls, and for ensuring, to the greatest possible extent, that USGS data is properly managed and that all access to USGS data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team within one hour of discovery in accordance with Federal policy and established procedures.