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: U.S. Geological Survey - USGS Service Desk

Date: June 15, 2017

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

Bureau/Office Contact Title: IT Specialist

Point of Contact
Email: dmclavel@usgs.gov
First Name: Deborah
M.I.: M
Last Name: Clavel
Phone: (303) 236-6146
Address Line 1: Box 25046, Mail Stop 801
Address Line 2: Denver Federal Center
City: Lakewood
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) Service Desk is the single point of contact for technical and support issues for approximately 8,000 USGS staff, administrators, managers, and scientists. The USGS Service Desk's vision is to deliver on-demand, world-class services and solutions.

The USGS Service Desk's mission is to:

- Enable USGS science by taking ownership of each service request
- Manage each request correctly
- Escalate efficiently
- Communicate to the customer
- Ensure customer satisfaction

The USGS Service Desk utilizes two information technology (IT) solutions: 1) Remedy and 2) Bomgar.

Remedy is a ticketing system used to track IT service requests, incidents, problems, infrastructure change requests, and other business service management data.

Bomgar is a remote support solution that allows IT support technicians to remotely connect to end-user systems for the purpose of troubleshooting end-user technical issues.

C. What is the legal authority?

43 U.S.C. 31 et seq. The Organic Act of March 3, 1879, as amended (1962); directs the Geological Survey to classify the public lands and examine the geological structure, mineral resources, and products within and outside the national domain.

5 U.S.C. 301, 3101, 5105–5115, 5501– 5516, 5701–5709; 31 U.S.C. 66a, 240– 243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Executive Order 11807.

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*

E. Is this information system registered in CSAM?

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

010-000001013 System Security Plan for Science & Support Systems

☐ 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.*
Remedy	To create and track USGS Service Desk service requests	Yes	Remedy pulls information from Active Directory including names, email addresses, mailing addresses, and phone numbers. Additionally, personally identifiable information (PII) may be contained in tickets entered into the system by customers and technicians. Commonly, the PII entered into the system contains personal address; personal email address; personal phone number; computer name, including Internet Protocol (IP) address; and other computer information needed to troubleshoot problems. This additional PII is used to contact customers that need technical help but are not at their duty location.
Bomgar	To allow IT support	Yes	Bomgar video records

	technicians to connect to end-user systems for the purpose of troubleshooting end-user technical issues		remote support sessions and keeps the recordings for three months. The recordings may contain PII seen on a customer's computer screen. Bomgar automatically captures information about the customer's computer including IP address, computer name, memory, processor, etc. Additionally, Bomgar has a built-in chat feature that is also saved for three months. Customer may put PII into the chat including name, email addresses, mailing addresses, and phone numbers.

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)*

Employee Administrative Records - Interior, DOI-58

☐ No

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

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

I. 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
- ☐ 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
- ☒ Other: *Specify the PII collected.* IP Address, Active Directory Information, Computer System Information (Make, Model, Operating System, etc.)

A. 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*

B. 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: Bomgar Chat or screen recordings. Remedy tickets.

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

The intended use of the PII is to create and track service requests from individuals who contact the USGS Service Desk. The PII collected will only be used to contact customers and resolve service requests.

D. 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 PII will be shared with USGS personnel who have a need-to-know to resolve service requests. Personnel with a need-to-know may include IT technical support staff or officials designated to respond to certain incident types. For example, the Associate Privacy Officer may be designated to respond to privacy incidents, training leads may be designated to answer questions about annual training requirements, etc.

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

Other bureaus within the Department of the Interior (DOI) use Remedy and Bomgar. Remedy is used to track Electronic Serial Number change requests for all of the DOI. Additionally, Remedy is used to track Information Technology Security Incidents. All ticket information is restricted to the bureau and specific support team. Bomgar is used by several DOI bureaus. Each bureau can view Bomgar recording and chats from their own support teams only.

☐ 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.*

E. 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.*

Individuals may choose but are not required to provide personal contact information if working remotely. Non-sensitive PII is generally retrieved from existing systems to produce reports that are administrative in nature. For example, Active Directory information is contained within the system to streamline the incident reporting process and to allow support technicians to easily follow up with individuals who have open service requests.

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

F. 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: Bomgar provides a privacy notice as part of the initial connection. Remedy provides a privacy notice on the login screen. Most people do not see the login screen and single sign-on into Remedy. If single sign-on worked, the person is on a government computer and signed into an Active Directory authenticated account, so a privacy notice was provided at the time of logging into the government computer.

☐ Other: *Describe each applicable format.*

☐ None

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

Information is retrieved by incident identification (ID) number, name, and/or email address.

H. Will reports be produced on individuals?

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

Reports will be produced on individuals to track their service request histories. These reports document actions taken by support technicians to resolve service requests at each stage of the troubleshooting process: 1) identification and recording, 2) investigation and diagnosis, 3) resolution and recovery, 4) incident closure, and 5) closed.

☐ No

Section 3. Attributes of System Data

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

Not applicable; no information is collected outside the DOI network.

B. How will data be checked for completeness?

Data is checked for completeness by the individual providing the data and cross-referenced with existing USGS databases, such as Active Directory.

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

The data is updated yearly as required by an annual Assessment & Authorization review.

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

Records in this system are maintained under the USGS General Records Disposition Schedule (GRDS) 202-08 – IT Customer Service Files. GRDS 202-08 is a USGS-wide records schedule that covers records related to providing help desk information to customers; help desk logs, reports, and other files related to customer query and problem response; query monitoring and clearance; customer feedback records; and related trend analysis reporting. Records are destroyed when one year old or when superseded, obsolete, or no longer needed, whichever is later.

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

Hard copy records shall be shredded or pulped. Electronic records shall be deleted. Backup tapes are reinitialized and reused. Procedures are documented in section MP-06 of the Media Protection (MP) Standard Operating Procedures document.

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.

During all phases of the information lifecycle, the principle of least privilege is observed. Major potential privacy risks include inadvertent disclosure, unauthorized surveillance, and theft. Such disclosure could reveal details of an individual's IP address, contact information, and service request history. PII is stored and maintained on internal systems only. It is protected from unauthorized access by firewalls, intrusion detection systems, antivirus programs, and the inherent security of the Active Directory domain environment. To mitigate the insider threat, collected data is protected by a combination of user ID, user password, and limited restricted access. Employees are required to complete the yearly Information Management and Technology (IMT) Awareness Training, which includes affirming the USGS Rules of Behavior. Audit logs for the data are reviewed regularly for anomalies. The data is not shared outside

the USGS/DOI. USGS computers are secured and scanned monthly in accordance with the USGS Continuous Monitoring Program Plan.

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*

The data collected is only used to create and track service requests and to follow up with individuals if more information is needed.

☐ 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; this system 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* Officials Delegated to Handle Certain Incident Types

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

Access will be obtained only by those whose names are on the access control lists of the system. Access to the data is determined by an individual's need-to-know, job description, and decision of the USGS Service Desk Chief. Criteria, procedures, controls, and responsibilities regarding access are documented by those responsible for the data. Users can see Remedy tickets in their name but cannot edit the information.

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?*

Privacy Act. The Contractor staff shall be familiar with and adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. If, while in performance of this PWS, access to this type of information is required, Contractor shall use this information for Contractor's designated project only.

52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

☐ 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. Individuals have to identify themselves to receive support. Although the system is not designed to locate individuals, Bomgar provides remote viewing/monitoring of the customer's computer and captures IP addresses. The IP address could be used to determine the approximate location of the customer.

☐ No

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

Active Directory information is collected as a function of the monitoring of individuals, which includes office location and work contact information. IP addresses and other PII is collected that could allow locating individuals. Additonally, Bomgar allows viewing and recording of an individuals computer.

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

Access control lists restrict access to authorized users. Privacy Act Warning Notices are posted in appropriate locations. Electronic systems are protected from unauthorized access by firewalls, intrusion detection systems, antivirus programs, and the inherent security of the Active Directory domain environment. To mitigate the insider threat, collected data is protected by a combination of user ID, user password, and limited restricted access. Employees are required to complete the yearly IMT Awareness Training, which includes affirming the USGS Rules of Behavior. Audit logs for the data are reviewed regularly for anomalies. The data is not shared outside the USGS/DOI. USGS computers are secured and scanned monthly in accordance with the USGS Continuous Monitoring Program Plan.

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 USGS Service Desk Chief serves as the Information System Owner and the official responsible for oversight and management of the USGS Service Desk security and privacy controls, including the protection of information processed and stored by the USGS Service Desk program. The Information System Owner and the Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by the USGS Service Desk program. The System Manager is responsible for protecting the privacy rights of the public and employees 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 Information System Owner is responsible for oversight and management of the USGS Service Desk's security and privacy controls and for ensuring, to the greatest possible extent, that agency data is properly managed and that all access to agency 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, preferably by the assigned Security Point of Contact, within one hour of discovery in accordance with Federal policy and established procedures.