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: IT Service Management System (Remedy)
Bureau/Office: Office of the Chief Information Officer
Date: March 10, 2020
Point of Contact
Name: Danna Mingo
Title: OS Associate Privacy Officer
Email: os_privacy@ios.doi.gov
Phone: (202) 208-3368
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a PIA required?

☒ Yes, information is collected from or maintained on

- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☒ Volunteers
- ☐ All
- ☒ Other: Vendors and Indian Tribes

☐ 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?

Remedy is a software and web-based IT Service Management application system deployed on the premise of the Department of the Interior (DOI) to provide a framework for storing, accessing, and managing DOI incidents, changes and work orders through the use of consistent processes. Remedy supports the lines of business that include Business Service, Financial Service, and IT service. Remedy not only processes customer requests for the Office of Human Resources (HRD) and Financial Management Division (FMD) within the Interior Business Center (IBC) of DOI, but also supports the Federal agency customers whom the IBC provides shared services to. Remedy also includes and supports the DOI Cyber Incident Response Center (DOI-CIRC), DOI's enterprise-wide security incident reporting activities.

The DOI Office of the Chief Information Officer (OCIO) is responsible for managing and maintaining the Remedy system. The Customer Support Center (CSC), Service Delivery Division within the OCIO uses Remedy to capture and process all change requests, incident and problem reports, to provide support to the lines of business applications for incident management, the Change Management for managing infrastructure changes, the Asset Management for data center inventory tracking and infrastructure management, and the Service Request Management.

Remedy enables DOI to automate and process customer needs to improve business processes and optimize the deployment of solutions and resources. Remedy is hosted in the OCIO Data Center Boundary and consists of the following modules:

- Incident and Problem Management -The Incident module is a ticketing system for reporting, tracking and resolving customer issues and requests for supported applications, products and services, including DOI cyber security incident tracking service. It provides an environment to efficiently handle the logging of incidents within Tier 1 and Tier 2 levels of support. The Problem Management module is also a ticketing system that provides a structure for identifying underlying problems. Its purpose is to prevent recurring issues from happening by identifying the root cause and known errors.

- Work Order Management - Automated work assignment for processing customer requests.

- Asset Configuration Management - Manages IT assets to support system management. Assets include items such as servers, network devices, storage solutions, software, etc. A key objective is to identify those resources so the business can maintain plans to replace old equipment, charge customers for dedicated and shared equipment.

- Change and Release Management - Manages changes in the IT hosting environment and the IT infrastructure (e.g. host, network or databases). The Change Manager uses Remedy to record, maintain, and track the routing of the change request, including the review, authorization, implementation and completion processes. The Release Management subsystem is installed but not in use at this time.

- Service Request and Work Order Management - Data collection web interface for users to enter service requests into the Remedy system. Data collection from this interface is then mapped into an Incident, Work Order or change Request for fulfillment in Remedy. Work orders are generally used to send the fulfillment directly to the team to perform the work.

- Service Level Management - Measures Service Levels within the system for response and closure of incidents. Remedy allows targets (timeframe for resolution) to be set for different types of issues or problems. The system will measure if that particular issue has been resolved in the agreed timeframe.

- Knowledge Management - Access point that contains Remedy resources and allows users to search the Remedy database for incidents, guides, or work instructions.

- Discovery Tool - Scans DOI network and collects information needed for asset management.

- SmartIT & Smart Reporting - SmartIT provides a GUI look and feel interface to Remedy applications. Smart Reporting is a Remedy reporting environment.

- Digital workplace (MyIT) - BMC Software (BMC) Digital Workplace is a self-service application for business users to connect with IT and HR anywhere, anytime, on any device. Users are encouraged to share their experiences and post status updates about the resources that concern them. IT can analyze the conversations around resources to gain insight into service usage trends, in order to plan for the organization's future needs more efficiently, etc.

C. What is the legal authority?

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, “Streamlining Service Delivery and Improving Customer Service”, April 11, 2011; Presidential Memorandum, “Security Authorization of Information Systems in Cloud Computing Environments”, December 8, 2011; Presidential Memorandum, “Building a 21st Century Digital Government”, May 23, 2012.

44 U.S.C. §§ 3551-3558, Federal Information Security Modernization Act (FISMA) of 2014; E-Government Act of 2002; OMB Memorandum: Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirement, M-16-03 of 2015; Presidential Policy Directive (PPD)-41, United States Cyber Incident Coordination, July 26, 2016; Department of Homeland Security directives; National Institutes of Standards and Technology (NIST) Special publication 800-61, Computer Security Incident Handling guide; OCIO Memorandum - 01-12-2009 - Electronics Records Management and Preservation; OCIO Memorandum - 02-15-2013 - Managing Federal Records for Departing Political Employees; US-CERT Federal Incident Notification Guidelines.

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*

010-000002539; Remedy SSP

☐ 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	N/A	N/A	N/A

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)*
☒ No

Remedy is a customer service and help desk ticketing system, and is not the official system of record, however, it is an internal system which supports numerous DOI HR, financial and other systems including: DOI Enterprise Service Network (ESN), DOI FPPS, FPPS Datamart, DOI Talent, eStaffing, EODS, Quicktime, TMS/FedTalent, WebTA, WTTS, E2Solutions, FM Travel(CGE), FBMS, Travel-CGE, OFF, TIPS, IMARS, and the DOI-CIRC security incident reporting portal. The DOI records in the systems of records are maintained by the DOI system managers under government-wide and DOI system of records notices, which may be viewed at https://www.doi.gov/privacy/sorn, as well as system of records notices published by external agency customers who own the data that is being processed by DOI.

- OPM/GOVT-1, General Personnel Records, Records, December 11, 2012 (77 FR 73694); modification published November 30, 2015 (80 FR 74815)
- GSA/GOVT-3: Travel Charge Card Program, April 3, 2013 (78 FR 20108)
- GSA/GOVT-4, Contracted Travel Service Program, June 3, 2009 (74 FR 26700)
- DOI-45, HSPD-12: Identity Management System and Personnel Security Files, March 12, 2007 (72 FR 11036)
- DOI-16, Learning Management System, October 9, 2018 (83 FR 50682) - manage Department-wide training and learning programs
- DOI-10, Incident Management, Analysis and Reporting System, June 3, 2014 (79 FR 31974)
- DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - March 12, 2007 (72 FR 11040)
- DOI-85, Payroll, Attendance, Retirement, and Leave Records, July 19, 2018 (83 FR 34156)
- DOI-86, Accounts Receivable: FBMS, July 28, 2008 (73 FR 43772)
- DOI-87, Acquisition of Goods and Services: FBMS, July 28, 2008 (73 FR 43766)
- DOI-88, Travel Management: FBMS, July 28, 2008 (73 FR 43769)
- DOI-89, Grants and Cooperative Agreements: FBMS, July 28, 2008 (73 FR 43775)
- DOI-91, Oracle Federal Financials, September 10, 2013 (78 FR 55284)

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

☐ Yes: *Describe*
☒ No

Per the Information Collection Clearance Officer & Departmental Forms Manager: “These information collections do not trigger the PRA because they are internal and the information is collected from Federal government employees acting within their duties.”

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

The CSC discontinued loading PII related information and forms into Remedy at the end of FY 2014. Since that date, the CSC no longer allows PII related forms to be uploaded as an attachment in Remedy. Standard procedures have been developed in order to process forms and are no longer tracked and/or processed in Remedy. Forms that are submitted to the Helpdesk are not processed in Remedy and will be forwarded to the appropriate POC for processing.

As marked above, PII data that is collected is required for business purposes when providing assistance to the customers.

- Personal Cell Telephone Number, Personal Email Address, Home Telephone Number: The CSC collects this contact information to communicate with former employees when a business need requires it.
- Mailing/Home Address: The CSC only collects parts of the address that needs to be updated as provided in the request. For example, "Please update zip code to 80220" or "Correct street to 'lost lake lane' instead of 'lost lake place'."
- Child or Dependent Information: When Child or Dependent changes are requested, the CSC only collects Child or Dependent information as it pertains to a specific Child Support issue or payment, and does not add the names of the Dependent or Children to the ticket.
- Military Status/Service: When Military Service status is referenced, the CSC only collects the customer's military status in relation to their military service. For example, "Customer is on Military Leave and has not received his Leave and Earnings Statement".
- Employment Information – This information is collected only as it pertains to an employee's Bureau/Office or Company for ticket management assignment purposes.

Remedy supports numerous agency customers and the PII types vary by customer and line of business. Customer data in Remedy is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act. Remedy CSC staff access customer data to provide support to each customer and only have limited access as determined by the customer agency.

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

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

Contractors, Volunteers, and Vendors

Some PII information is collected from the various security tools used for cybersecurity reporting and security incident investigation. This data is maintained in the DOI-CIRC portal and other security monitoring systems, and is not stored in Remedy. Please refer to the DOI Information Assurance Enterprise Application Environment (IAEAE) PIA for more information.

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

☒ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Website
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems: *Describe*

Remedy supports FBMS customers through the FBMS Portal Integration which provides authorized portal user with web service access to Remedy to create helpdesk tickets and view the status of the tickets submitted. Each FBMS customer has a FBMS Reporting Integration Remedy Account interface allows FBMS to have direct access to the Remedy reporting database for the purpose of creating and refreshing visualizations and analysis. The Business Integration Office (BIO) with access to FBMS have only access to the view of Remedy Ticket Information. There is no interface connections between Remedy and other systems/applications that Remedy supports. Remedy CSC Tier 1 service personnel would access the systems that Remedy supports to manually pull data for the purposes of data validation, they would not change or store the data.

DOI internal user profile information are initially set up through DOI Active Directory service, which Remedy is synchronized with.

☒ Other: *Describe*

The customer contact information is collected and entered into Remedy so as to be referred to the appropriate office for action when the customer submits requests to CSC Help Desk. The customers can call, or email, or fax to report issues to the help desk, or they can submit requests through the website.

Fax, Email and attachment:
The CSC works with the customer to resolve the issue and is responsible for updating and closing the ticket, documenting any actions taken, and providing a description of the resolution. One of the features that assists support staff with the tickets is an email integration capability within the incident management application that automatically converts incoming emails including documents attached in the customer's email to incident requests. In addition, the CSC will review the tickets/requests and forms/attachments submitted by the automated email system for PII data. If the form or email contains PII data then the PII data will be removed from the Remedy system and the form will be processed externally through fax and blue envelope.

Website:
Information may also be provided through the Remedy Service Request Management internal web interface. Service Request Management provides an online user self-service interface from which employees can view and request services that are available to them. This is one of the self-service automated processes that DOI OCIO develops to assist the customers with requesting services without having to go directly to the Help Desk.

Information is manually retrieved/verified by help desk staff from the systems that Remedy supports to research and document the customer request. Help Desk personnel have read access to many systems supported by the Customer Service center to assist the customers with their requests. In some limited cases, the Help Desk personnel have write access to designated applications. For the remaining customer access to systems, the Help Desk uses Bomgar to remote into machines.

Phone call:
Any user can call the help desk to open an Incident. Remedy syncs with DOI Active Directory (AD) to build customer accounts for DOI users. In the rare event the users aren't in the system then the CSC adds a customer profile record for them. This is also true for forms submission for DOI users. A user fills out a form and their supervisor authorizes it to be submitted to the CSC. There are many forms used by the OCIO and DOI bureaus, such as the form for IT system access, application requests, travel, etc. Forms with PII are faxed to the CSC.

Information Shared Between Systems:
Remedy People Profiles are synchronized with DOI Active Directory using the Lightweight Directory Access Protocol over SSL (LDAPS). The query used against Active Directory searches the Global Catalog (across domains) for enabled user accounts that have an email address associated with it. The query filters out elevated privilege accounts, contact records, and service accounts. The integration performs some data manipulation activities instream before the data is imported into a staging form with the Remedy application. Workflow on this staging form determines if a Remedy profile already exists, the workflow performs some minor updates. If no profile exists, it generates a read only Remedy account that allows the user to access the Remedy Service Request Management (SRM) self-service application.

Information sharing within Remedy system:
The Remedy modules use the same database and can access the table of data relevant to the operation of a specific module. This is a critical and necessary aspect to providing full IT Service Management capability. Users are assigned roles in the system and these are assigned by the Remedy module the user may need access to. The users are always given the least privilege necessary for the user to perform their job function. For example, a customer calls into the Customer Support Center with a laptop issue. The laptop is stored in the remedy asset management module and can be linked to the incident and associated to the customer so all data is aggregated together for the customer. Another example could be that multiple people are affected by the same issue so multiple incidents get created, such as for a network outage. Because of the impact and the urgency associated with this the IT team decides that a problem needs to be created and associated to these incidents so that a root cause and solution can be identified to resolve the issue. Once the problem root cause and solution have been identified a

change request is necessary in order to implement the permanent fix. It is essential that these specifically identified limited dataset be shared between these modules.

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

The CSC discontinued loading PII related information and forms into Remedy at the end of FY 2014. Since that date, the CSC no longer allows PII related forms to be uploaded as an attachment in Remedy. Standard procedures have been developed in order to process forms and are no longer tracked and/or processed in Remedy. Forms that are submitted to the Helpdesk are not processed in Remedy and will be forwarded to the appropriate POC for processing.

Prior to the end of FY 2014, the Point of Contact Information such as the customer name, official email address, telework site address, or office work station were collected by Remedy Customer Service Center for issue resolution and follow-up purposes. Some other PII as the subject of the incidents might be submitted by the customers when reporting incident or requesting change to the existing PII collected and stored in the systems that Remedy supports. The incidents reported which might include some PII information are routed for resolution purposes to the Tier 2 administrators of the supported applications where the PII are originally maintained. For example, Travel Management has associated forms for user profiles which may contain PII data, such as birthdate, home city/state, last 4 of SSN, Employee ID, CGE login ID. The PII that Remedy processes for IT hosting, Financial Management and Human Resource lines of business are covered under government-wide and DOI Privacy Act system of records notices.

The PII is used for documenting and processing customer requests. Some sensitive PII may be found in attachments when users choose to provide or upload information so as to update their PII information in the systems that Remedy support.

The DOI-CIRC incident tracking function in Remedy is specifically designed with data privacy protection mechanism which does not allow attachments to be uploaded into Remedy. Attachments may be loaded from the custom form but a warning exists for the limited number of support personnel who have access to this form not to upload information containing PII.

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.*

PII provided by DOI agency customers are shared within the OCIO, the Office of the Secretary (OS), IBC, and the FBMS/Business Integration Office to process and resolve customer issues and requests and for tracking DOI Cyber Security incident reported.

Any user can call the help desk to open an Incident. If they aren't in the system then the CSC adds a customer service profile record for them. This is also true for DOI internal forms submission. A user fills out a form or submits a request through SRM, their supervisor would have access to the information disclosed in the form or SRM and authorizes the form to be submitted to the CSC. These forms that contain PII information are faxed to the CSC. The CSC then faxes the forms to the appropriate Tier 2 group for processing.

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

PII may be shared with other DOI bureaus and offices to process and resolve Tier 2 customer requests. HR forms may contain PII such as the last four of social security number, personal cell or personal email, birthdate, home address, etc. Tier 2 support includes configuration and network communication issues, application configuration issues, job scheduling, table maintenance, supplier information, application security, and issues escalated from Tier 1, as well as other complex issues. Currently, these forms containing PII are shared with CSC via fax. The CSC then faxes the form to the Tier 2 support team for processing.

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

Some specific PII of the employees of other federal agencies can be shared with Federal agency customers to resolve their employees' specific requests. This data is not stored in Remedy today. Reports are only shared upon request from the Federal agency customer. There is no PII data in the reports. The reports are reviewed and any PII are scrubbed before sharing.

The data collected for cyber security incident tracking purposes might be shared with those corresponding authorized personnel in other Federal agencies, such as Department of Homeland Security (DHS) US-CERT, as well as local and Federal law enforcement agencies with a "need-to-know" directly connected to the specific incident being processed.

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

Some specific PII can be shared with Tribal, or State agency customers to resolve their specific incident requests. Reports are only shared upon request from the Tribal, or State agency customers.

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

DOI contractor staff who provide support for the Remedy system and its customers have authorized access to Remedy system and data which are the subject of the issues in order to perform their duties.

The contractor personnel assigned to the DOI-CIRC team, DOI threat team, DOI enterprise messaging team, etc. with a need to know directly connected to the specific incident reported might have access to the data of the specific incident processed by Remedy support service.

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

The enhancement or replacement of DOI network devices or equipment necessitate the change management processes of Remedy. DOI vendors (currently Verizon) are authorized as DOI network users to access Remedy via DOIApps and will have a PIV card and authenticated on the DOI Network to complete the specific task through a DOI work order. Government Furnished Equipment (GFE) will be required for this access unless a waiver is granted from Security for the vendor to be allowed to use personal equipment.

Once the vendor is in the Remedy system they will be isolated to only the data they are allowed to see and manipulate within the system. They will be working assigned tasks in the Incident Management module to do technical analysis for circuit order requests. Emails are also a part of the communication which occurs with this process today between the vendor and other contacts. Verizon (external) emails as well as the internal emails will be integrated into the email automation project as part of the current email integration project.

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 requests for Remedy support are inbound requests to the CSC/IBC/OCIO. Individuals will need to submit their contact information to process requests as appropriate. Submission is voluntary, however, failure to submit requested information may result in delay of resolution of issues. Individuals have the option to select additional self-help and self-processing options within Employee Express external to Remedy for HR-related requests.

During the service process, the Remedy system might process incident information of its supported systems, including cyber security incident management and tracking tools. The privacy risks of these tools are assessed separately in the DOI IAEAE PIA. Please refer to DOI IAEAE PIA for more information in this regard.

☐ 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.*

Remedy collects information from individuals on behalf of agency customers. Access request forms and other forms generated by the DOI bureau/office customers, such as payroll forms, HR, and traveler profile forms with PII information, are owned and managed by bureaus/offices and program offices who are responsible for ensuring the forms are authorized to be used and that Privacy Act Statements are included in the approved forms that collect PII for applicable Privacy Act systems.

☒ Privacy Notice: *Describe each applicable format.*

Privacy Notice is also provided by this published Remedy PIA and the referenced SORNs and PIAs for the Privacy Act systems that are supported.

☒ Other: *Describe each applicable format.*

A Remedy Privacy Warning is placed at the Remedy URL login and collection sites where individual employee customers submit requests for assistance. DOI Privacy guidelines are provided where the DOI clients can retrieve for reference.

CSC employees may attach documents and enter work information for Tier 1 and Tier 2 customer requests. A statement is placed next to the "Attach" or "Upload" button to inform CSC employees not to upload documents that contain PII into Remedy: "To protect individual privacy, please do not upload documents that contain sensitive personally identifiable information."

☐ None

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

Data can be retrieved manually by individuals who are authorized to access the system. They can search by incident ticket number, customer name, reports generated by Remedy help desk and system support users or automatically for customers, and tickets assigned to the Tier 1 and Tier 2 application support users or groups.

Data for cybersecurity incident tracking can be retrieved by incident number, ticket number, ticket type, name of POC, date of incident or by doing a keyword search on any field within the database. The only way to query by name is for queries involving name of the creator of a ticket or the assigned POC of a ticket. The association of these names to incidents is in relation to their official government duties.

I. Will reports be produced on individuals?

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

Reports can be created and distributed for the purpose of training, workload reporting, volume reporting, projections, and other related reasons. In some cases reports will automatically run and be sent to external customers. The auto generated reports are for the application support personnel to use to support their IT, FM and HR applications. In some instances, information in the summary may contain PII not specifically required; however, the responsible staff members are instructed to review and sanitize reports to ensure PII is not entered. The CSC ensures any material and all training materials that require screen prints or any other real world case examples do not include PII. Reports may be shared with external customers; however, these

reports are reviewed by the lines of business to ensure PII is not included. When Reports are shared with external customers (non-support personnel), PII is not part of the reporting.
For cyber security incident tracking, reports are not produced on individuals but rather incidents.

☐ No

Section 3. Attributes of System Data

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

Remedy provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the Remedy system might trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information to properly address the inquiry and troubleshoot the payroll, HR or other customers issues and requests.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

B. How will data be checked for completeness?

Remedy provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the Remedy system would generally trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information to properly address the inquiry and troubleshoot the payroll, HR or other customers issues and requests properly. In addition, the Remedy Tier 1 and Tier 2 support staff ensures the incident and change request ticket is complete and all required information is entered or attached to resolve or escalate the customer request.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

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

Remedy provides support to many systems. The data in these systems are regularly updated to maintain the completeness, currency and accuracy. The use of the Remedy system would generally trigger identity and other information verification processes to reflect the completeness, currency and accuracy of the information so as to address the inquiry and troubleshoot the payroll, HR or other customer’s issues and requests properly. Data in Remedy, including attachments, may be manually verified with the systems/applications that the Remedy supports to ensure data is current, as needed, to resolve or escalate the customer request.

For investigation and forensic purposes, the cyber security incident tracking processes do not modify any data.

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

Official records maintained in the Remedy system are held in accordance with DOI's Administrative Departmental Records Schedule. Records of Business Services (for ordering property) are covered in Section 1, Short-term Administration Records (DAA-0048-2013-0001-0001). All others fall under Section 4, IT Information. Three areas within that section separate the records with retentions between 3 and 7 years. The sections are: System Maintenance and Use (DAA-0048-2013-0001-0013); System Planning, Design, and Documentation (DAA-0048-213-0001-0014); and Long-term Information Technology Records (DAA-0048-2013-0001-0015).

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

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. Records processed on behalf of the customers are maintained in customers systems and are covered under their applicable records retention schedules.

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

Remedy provides the framework for storing, accessing, and managing DOI incidents, problems, work orders, IT changes as well as asset inventory and supports many systems for DOI, including those that provide shared service to federal agencies customers, such as the Federal Personnel and Payroll System (FPPS) and FBMS, through the incident and change management processes. DOI also uses Remedy to record and track cyber security incidents using the DOI-CIRC process. The PII provided by the users of the Remedy system as the subject of the incidents or the POC information provided by users for follow-up of issue resolution are an inevitable part of the data that Remedy handles. There are moderate privacy risks for use of the Remedy system. Accordingly, DOI uses a series of administrative, technical and physical measures to ensure that adequate security and privacy controls are selected and put into place to mitigate these risks.

Even though the systems that Remedy support do not directly transfer PII into the Remedy system, there is a risk that the PII may be inadvertently entered into the Remedy system in the process of creating an incident ticket. DOI mitigates this risk with a statement that instructs users not to attach any files that might contain PII information not required for creating an incident ticket.

The Remedy tickets might reference records containing PII, however, Remedy does not collect nor process PII other than what the customers/data subjects already consented to provide to the government or to federal agency employers to fulfill their official duties. The PII is originally collected via proper Notice and Consent processes, such as publishing DOI Privacy Impact Assessments and DOI-wide or government-wide Systems of Record Notices, obtaining OMB approved form control numbers, and publishing Privacy Act Statements on the forms. To mitigate the risk of unauthorized disclosure or misuse of the PII, the CSC team has an established process that sanitizes the work reports CSC generates so as to ensure the reports will not contain PII. Data sharing is strictly for the purpose of issue resolution or incident tracking and for purposes as identified in this PIA. The customer data, including PII, will not be used for any other purposes, and will not be repurposed under any circumstances.

To properly segregate the information used for the Remedy asset management function, CSC pre-defines specific datasets used for this specific purpose and synchronizes it with the BMC discovery tool which stores agency protected information such as server name, IP address, server location, firewall data, etc. into the configuration management database (CMDB). As the result of this control, only the Incident module is used as the customer information collection point for forms and data, no information can be transferred between different modules.

Customer Service Center customers may also use the Service Request Management module, which offers an internal web portal for customers to report incidents or to request services. The ticket generated may contain unrequested PII data for the customers. To mitigate the relevant privacy risk, the CSC has a process to review all data to ensure the published documents do not contain PII data.

The specific Remedy supported processes of the DOI Enterprise Network System (ESN) originally handled by DOI Geological Service Remedy (USGS) are now merged and consolidated with OCIO Remedy. In addition, the supporting process for DOI Computer Incident Response Center (DOI-CIRC) process has been moved from the USGS Remedy system to the OCIO Remedy system. Accordingly, more data elements are being processed by OCIO Remedy, which include incident related information and might contain PII. To mitigate the risk for DOI-CIRC, the PII tab is protected/isolated from the incident itself. Only limited users have access to this information. Remedy has designed and implemented separate incident tracking and information display pages for DOI-CIRC and has also disabled the feature of uploading attachments on the main incident form so that no document containing PII can be unnecessarily shared and potentially stored in Remedy.

Twice a year, the Remedy system support personnel will employ database queries and reporting utilities to extract and review data that may match SSN data structure masks. This data will be reviewed and removed or masked in the system manually if determined that it contains PII.

To mitigate the risk of unauthorized access, access controls are implemented within the Remedy System ensuring the least privilege policy are enforced via inheriting the active directory controls from the Denver Data Center boundary, and the access control measures are being continuously monitored. Role-based access is manually reviewed and audited annually. Additional security measures have been designed and implemented to ensure that only DOI-

CIRC administrators, DOI-CIRC bureau users, and Privacy officials can access DOI-CIRC incidents within OCIO Remedy. Additionally, users from each bureau are only entitled to view tickets associated to the bureau in which they are assigned. The Remedy incident tracking process for DOI-CIRC also documents and tracks the reported incident information collected by Encase - a forensic tool used for incident investigation. Encase can capture any data of interest residing on a user's computer system, however, these data are not stored in Remedy; and have been provided adequate security and privacy controls under the DOI security program.
To ensure the Remedy records are maintained and disposed of in compliance with the U.S. legal requirements, various record retention and disposition schedules are identified for specific sets of records of Remedy. DOI properly defined and assigned roles and responsibilities for the record management and has established record retention and disposition procedures, policy and departmental manual for DOI personnel to follow, thereby mitigate the potential risks that might arise from mishandling of Remedy records.

To maintain its compliance environment and posture, DOI requires its employees and contractors to complete security and privacy awareness training during on-boarding. All DOI employees and contractors are required to complete annual Security Awareness Training, Privacy and Record Management training, which is tracked and monitored in a training database. The DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training and sign DOI Rules of Behavior.

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 use of the data is relevant and necessary to provide support to the lines of businesses to process and resolve customer requests in a timely and efficient manner.

☐ 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?

Remedy 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 Administrators
☒ Other: *Describe*

Remedy uses a three tier approach to respond to the customer requests, all incident tickets are triaged by the Remedy Tier 1 helpdesk support staff, by either addressing the issue or routing it to Tier 2 support in the Business Integration Office (BIO):

Tier 1 Support: This is the Customer Service Center who provides first level of support to end-user to obtain incident resolution information. This support covers basic issues such as password resets, software navigation issues, troubleshooting standard software functionality issues, system availability checks/validations, and workflow errors and updates. Issues requiring more extensive expertise are escalated for Tier 2 support. During the escalation and resolution process, customers can contact the Customer Service Center Help Desk for a status update or other concerns regarding the incident. Customer POC information such as the name, and email address are collected for issue resolution and follow-up purpose. Once the incident is created, it is then assigned to the appropriate Tier 2 support team for resolution

Tier 2 Support: The Tier 2 support is provided by application administrators for the applications identified previously. This support covers configuration and network communication issues, application configuration issues, job scheduling, table maintenance, supplier information, application security, issues escalated from Tier 1, or customer requests, such as a missing W2 as well as other complex issues. The Tier 2 support escalates issues requiring more extensive expertise to the Tier 3 support.

Tier 3 Support: The Tier 3 support requires coordination and interaction with the technical representatives in OCIO, IBC, FBMS and supporting vendors. Requires in-depth analysis and resolution of application or system problems. Remedy administrator also provide Tier 3 support for the Remedy application itself when issues with the Remedy system occur and for administration of the Remedy system.

Remedy administrator are the system administrators of the Remedy IT Service Management system and are responsible for system maintenance and upkeep, code development and deployment and user administration.

User access is determined by roles in the system. System administrators maintain the system and assign the roles and permissions and are responsible for the development efforts for the system. Tier1 (CSC agents) are given a role profile necessary to do their jobs across multiple applications they support. Tier 2 (Support Staff) are given roles to support their particular application/line of business and are placed in support groups to perform these roles.

The Remedy users have limited access to the system and are allowed to only submit requests into the system with read-only rights. The customer agency supervisor-level employees and the application support leads approve new user to be setup on the Remedy system. Tier 2 managers responsible for application areas such as FBMS authorize the addition of new users in the Remedy system as well as changes in Remedy which affect their areas of responsibility. The access rights of Tier 2 users require additional levels of approval.

Contractors provide Tier1 and Tier 2 support across the system have the same access rights as the government employees and are subjected to the same authorization and approval process. The Remedy team administers and develops automated solutions to improve customers processes. The Remedy team has contractors on board who perform development and maintenance of the system. All changes made by the contractors are reviewed and authorized by responsible government employees.

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

All the modules of the Remedy system share the same database and are closely integrated. The user access to the information can only be authorized based on the business need-to-know and least privilege and is constrained by the specific roles of the users. The Remedy system uses role level security. Users are granted access based on their specific role within the system for the user organization.

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?*

BMC is the vendor who provides the Remedy software and technical support to the Remedy team. BMC does not directly access the system, they do however provide direction on development of custom code and maintenance of the system. DOI has a contract with BMC for this ongoing support. The contractor is subject to the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1 and 24.2) and the specified contract clauses (Parts 52.224-1 and 52.224-2) to ensure that personal information processed or maintained by contractors who work on DOI-owned systems of records and the system data are protected as mandated.

Additionally, the following would apply to any contractor of the Federal Government:

- The Privacy Act applies to federal government contractors who operate systems of records containing personal information.
- When an agency contracts for the design, operation, maintenance, or use of systems containing information covered by the Privacy Act, the contractor and its employees are considered employees of that agency and are subject to the same requirements for safeguarding information as Federal employees.
- The contractors and their employees also are subject to civil and criminal sanctions under the Act for any violation that may occur due to oversight or negligence.

Remedy administrator contractors as well as Tier1 and Tier2 support personnel are subject to the same rules and regulations as government employees.

☐ 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*

System maintains audit logs of actions of the users in the system.

☐ No

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

Login, failed login, login date, actions in the system and changes such as the changes to a record for Tier 1 and Tier 2 staff are recorded in an application audit log.

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

Access controls are implemented to comply with the least privilege policy to prevent unauthorized monitoring, as inherited by active directory controls that reside within the OCIO Data Center. Levels of access are manually reviewed annually to ensure appropriate access for users dependent on their role. System access is controlled through roles and permissions within the application. The system administrator users must have a license and permission to view audit log information. Typically, all Tier 1 and Tier 2 support personnel can review the audit log information.

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 Hosting Services Chief, Service Delivery Division, Office of the Chief Information Officer serves as the Remedy System Owner and the official responsible for oversight and management of the Remedy security controls and the protection of customer agency information processed and stored by the Remedy system.

The Information System Owner and data owners 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 in Remedy and accessed by authorized staff in the supporting systems. They are also responsible for protecting the privacy rights of the employees and volunteer workers for the information they collect, maintain, and use in the system. The Privacy Act System Managers and data owners for the supported Privacy Act systems are responsible for meeting the requirements of the Privacy Act, providing adequate notice, making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with appropriate Privacy Officials.

Customer agency data in Remedy is under the control of each customer, and the customer agency is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, 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.

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 Hosting Service Chief, Service Delivery Division, Office of the Chief Information Officer has responsibility for daily operational oversight and management of the Remedy's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Remedy Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, within 1- hour of discovery in accordance with Federal policy and established DOI procedures, and that appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the appropriate Privacy Officials.