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: Virtual Employee Network (VEN)

Bureau/Office: Department of the Interior Offices (DO)/Interior Business Center (IBC)
Date: September 15, 2021

Point of Contact:
Name: Danna Mingo
Title: DOI Departmental Offices Associate Privacy Officer
Email: Danna_Mingo@ios.doi.gov
Phone: (202) 441-5504
Address: 1849 C Street, NW, Mail Stop 7112 MIB, Washington, DC 20240

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:

B. What is the purpose of the system?

The Virtual Employee Network (VEN) is a customized web application developed and managed by Relocation Management Worldwide (RMW). It is a relocation software and

automation technology tool developed for the Federal government's permanent change of station (PCS) programs as a transportation, delivery and relocation solutions service.

VEN provides full paperless automation for the entitlement or benefits ePolicy process. The system also manages and supports employee relocation processes including individual relocation requests and authorizations, funding obligations, and tracking of relocation events.

The Department of the Interior (DOI) Interior Business Center (IBC), Financial Management Directorate (FMD) uses VEN as an online web-based paperless solution to complete PCS moves, and track, manage and report on the relocation programs for IBC's internal and external Federal agency customers. VEN will enable IBC to implement additional paperless processes and remove redundant processes to ensure a comprehensive and efficient relocation service for IBC's Federal agency customers.

VEN software, technology tools and services are obtained through a General Services Administration (GSA) Multiple Award Schedule (MAS) 541511t - Transportation, Delivery and Relocation Solutions, and CHAMP program to automate the PCS service, track, manage, and report on the relocation programs, which complements the functionality of the DOI Financial and Business Management System (FBMS). As a GSA approved application, VEN meets all Federal Travel Regulation (FTR) requirements for full compliance with new technology and reporting requirements.

C. What is the legal authority?

5 U.S.C. Chapter 57, Travel, Transportation, and Subsistence; 26 U.S.C. 6011(b), Identification of Taxpayer; 26 U.S.C. 6109, Identifying numbers; 41 CFR Chapters 300-304, Federal Travel Regulation System; Federal Property Management Regulation (FPMR) 101-7, Federal Travel Regulations; E.O. 11609, Delegating certain functions vested in the President to other officers of the Government; E.O. 11012, Providing for the performance of certain functions under sections 1(a) and 1(b) of the Administrative Expenses Act of 1946; E.O. 9397, Numbering System for Federal Accounts Relating to Individual Persons; E.O. 13478, Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers; and DOI Permanent Change of Station Policy, which supplements 43 CFR Chapter 302, Relocation Allowances.

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:

E. Is this information system registered in CSAM?

☒ Yes:

UII Code:010-999991141
SSP Name: Virtual Employee Network.

☐ 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	**None**	N/A	N/A

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

☒ Yes:

GSA/GOVT-4 Contracted Travel Service Program, June 12, 2009, 74 FR 28048
DOI-88 Travel Management: FBMS, July 28, 2008, 73 FR 43769

☐ No

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

☐ Yes:
☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Gender
☒ Spouse Information
☒ Birth Date
☒ Financial Information
☒ Personal Email Address
☒ Marital Status
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other:

VEN collects the Travel Authorization (TA) number, which is assigned by the FBMS system when the IBC PCS Section Coordinator (Coordinator) enters the information taken from the relocating employee's Department of Interior Request for PCS Travel Authorization for Transferee Questionnaire (Questionnaire) into the system. This Questionnaire must be completed by the transferee to prepare the travel authorization and develop an estimate of the cost to the government for the transfer. FBMS generates a vendor code that is entered into VEN. This code is the employee's personal identifier number which follows the employee from agency to agency. The system also collects the reference tracking number, which is assigned to a specific relocation for each move. RMW assigns the Trans ID (Order Number) and the Government Bill of Lading (GBL) information for the VEN system. VEN utilizes single sign on and multi-factor authentication for system access, and issues usernames and passwords to relocating employees without a PIV card.

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:

The Federal agency customer contact submits a Request for PCS Coordination Form and a copy of the offer letter to the Coordinator when an employee is offered a position and requires relocation benefits. The Coordinator will send the Questionnaire and the DOI Employee Relocation Agreement and Disclosure Statement – Continental United States (CONUS) Move (Employee Agreement Form) to the relocating employee for them to complete and return. The Coordinator will counsel the relocating employee on all aspects of their move and create a TA number in FBMS. If the relocating employee requires temporary quarters or a house hunting trip in addition to the entitlements, the information about their name, address, number of vehicles, and the mileage driven will be entered into the VEN system. The entitlements for a transferee may include house hunting trip, temporary quarters subsistence allowance, en-route travel, miscellaneous expenses, real estate, evacuation, relocation income tax allowance, and shipment and storage of household goods. Employee vehicle license tag information is not collected or required for the relocation.

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:

Users can enter the relocation information into the VEN system. User access is managed by RMW and requires a PIV card or multi-factor authentication. IBC PCS collects the completed Questionnaire and the Employee Agreement Form through email sent by the relocating employee. After receiving these documents, the Coordinators will call the employee to review their entitlements and options. If the employee is not in the FBMS system, the Coordinator will forward the FBMS Customer Request Form for the employee to complete to generate the employee's vendor code. The Social Security number (SSN) in the FBMS Customer Request Form is no longer used as an identifier number; therefore, the field is manually wiped out before form is sent to the employee. The employee banking information in the FBMS Customer Request Form that is returned to IBC PCS is not entered into VEN or the FBMS systems. The completed FBMS Customer Request Form is forwarded via encrypted email to the IBC's Federal agency customer's representative to get the vendor code from FBMS. The relocating employee will submit via VEN, a completed Optional Form (OF 1012) Travel Voucher to IBC PCS

which is signed by the immediate supervisor and attach any receipts to claim for reimbursement of expenses incurred during the relocation. Employees that relocated prior to VEN coming online may submit vouchers through email, fax or regular mail. The PCS Accounting Technician receives the Travel Voucher via VEN or other means mentioned above and reviews the voucher for accuracy. The reviewed voucher is prepared for certification and is forwarded to the IBC certifying official. The voucher is then certified by the PCS Certifying Official and uploaded to FBMS and the Electronic Content System. Again, the SSN is not required from the employee and is never collected. The employee's name and address are entered into the VEN system. Any PII information shown on the vouchers in FBMS, such as employee name, address, and SSN can only be viewed or accessed by authorized PCS employees, and the RMW contractor does not have access to employee SSNs.

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

The PII collected is used to validate each employee's employment status and needed to process payments via accounting systems. It also is needed to provide counseling service to the employee about the relocation process and any related policy entitlements, make arrangements with the third party carriers for the relocation, process requests and vouchers, and report the activities to GSA. The PII will assist IBC in tracking, managing and reporting the relocation programs for IBC internal and external Federal agency customers.

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

☒ Within the Bureau/Office:

PII is shared within the IBC to initiate the PCS move. The Coordinators use PII (No SSN) to enter a request into the VEN system when the shipment and storage is requested, and to help the relocating employee throughout the entire relocation process.

☒ Other Bureaus/Offices:

The PII of bureau/office Federal employees are shared with bureau/office contacts who approve travel authorizations and travel vouchers. These bureaus/offices include the Bureau of Indian Affairs, Bureau of Reclamation, U.S. Fish and Wildlife Service Region 2, 3, 5, 7, and 9, and the National Park Service Washington Office (WASO), Intermountain, North East, South East, and Capital Regions.

☒ Other Federal Agencies:

The PII of Federal employees working for IBC's Federal agency customers are shared with the agency contacts to approve travel authorizations and travel vouchers. These Federal agency customers include American Battle Monuments Commission, Equal Employment Opportunity Commission, Federal Trade Commission, Millennium Challenge Corporation, National Transportation Safety Board, and Small Business Administration.

GSA requires IBC PCS to fill GSA 3080 Form - Household Goods Carrier Evaluation Report and send copies of all GBL vouchers processed to GSA on a monthly basis for GSA to audit what have been paid and processed as a safeguard against possible errors. Hard copies of the documents are sent via FedEx to the GSA office located in Washington, D.C.

☐ Tribal, State or Local Agencies:

☒ Contractor:

RMW, Armstrong Relocation Company and Commercial Relocation Services, Inc. (ARMT/RMW/CRS) and IBC signed a "Memorandum of Agreement for the Performances of Move Management Services, for Household Good Shipments, Facility On-Site Office Moves, Facility Off-Site Office Relocations, New Office Installations, and Office De-installations (MOA)". ARMT/RMW/CRS shares PII to carry out the contractual duties.

☒ Other Third-Party Sources:

RMW, Armstrong Relocation Company and Commercial Relocation Services, Inc. (ARMT/RMW/CRS) are the party with whom IBC signs "Memorandum of Agreement for the Performances of Move Management Services, for Household Good Shipments, Facility On-Site Office Moves, Facility Off-Site Office Relocations, New Office Installations, and Office Deinstallations (MOA)". ARMT/RMW/CRS shares PII with third party vendors to carry out contractual duties.

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

☒ Yes:

Employees voluntarily request and provide information for the service, and may decline services offered. The Coordinator will send the employee the Questionnaire and a copy of the Employee Agreement letter after the Coordinator receives the Request for PCS Coordination Form. At that time, the relocating employee can decline all relocation services even though they are still filling the position. If the employee declines to provide

the personal information needed; the relocation process will halt. The employee is advised to send an email declining the services or for providing the requested information for recordkeeping purposes. The Federal agency customer representative is notified that a travel authorization will not be generated. The file will be closed at that time and no data is entered into the FBMS or VEN systems.

☐ No:

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

☒ Privacy Act Statement:

Privacy Act Statements are provided on the various forms completed by employees.

- SF 1012: Travel Voucher Form
- GSA 3080 Form: Household Goods Carrier Evaluation Report
- Department of the Interior Request for PCS Travel Authorization for TRANSFEREE Questionnaire
- Request for PCS Coordination
- Employee Relocation Agreement and Disclosure Statement – Outside Continental United States (CONUS) Move

☐ Privacy Notice:

☒ Other:

There is a Terms of Use and Privacy Policy posted on RMW's website http://www.relocationmw.com where VEN can be accessed. Privacy notice is also provided through the publication of this PIA and the related Privacy Act SORNs that cover travel and relocation activities.

DOI PIAs and SORNs may be viewed on the DOI Privacy Program website at https://www.doi.gov/privacy/privacy-program.

☐ 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 will be retrieved by using identifiers such as name, Trans ID (Order Number), and GBL number. IBC PCS employees can access the VEN system using Single Sign On

(SSO) with their PIV credentials. Reports can be retrieved by entering the employee's last name in a search query, which generates a list of the relocated employees and can be further selected to view the employee information. These reports can be viewed or printed.

I. Will reports be produced on individuals?

☒ Yes:

System Internal Reports containing the employee name will be generated for tracking the status, storage, claim, invoice, and audit of the relocation. This report is accessible by RMW administrators and counselors, and IBC PCS coordinators and managers.

☐ No

Section 3. Attributes of System Data

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

The relocating employee is responsible for providing accurate contact information for the relocation. The Coordinator will review the information received from the relocating employee with the employee before any TA is created or entered into FBMS or VEN systems. In addition, the Questionnaire and Employee Agreement Form returned to the Coordinator requires the employee's signature to validate that the information provided in the documents is correct.

B. How will data be checked for completeness?

The Coordinator will review the information received from the relocating employee with the employee before any TA is created or entered into FBMS or VEN systems. In addition, the Questionnaire and Employee Agreement Form returned to the Coordinator requires the employee's signature to validate that the information provided in the documents is correct and complete.

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

Throughout the milestones of the relocation, the relocating employee will update their information on the original order form through the RMW counselors and IBC PCS Coordinators. The change history of the data is recorded on the VEN system through the RMW website at www.relocationmw.com, which shows dates of entry and the name of

the person responsible for the change. This allows anyone with authorized access to view notes or changes made to the relocation.

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

Records maintained in VEN are retained in accordance with the Departmental Records Schedule (DRS) approved by the National Archives and Records Administration (NARA). The VEN records are covered under DRS 1.3B, Long-Term Financial and Acquisition Records (DAA-0048-2013-0001-0011). These records have a temporary disposition and cut-off at the end of the fiscal year in which files are closed. Records are destroyed seven years after cut-off. The Records Destruction Request is completed by IBC personnel and authorized by the OS Records Management office.

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

DOI records are disposed of by shredding paper records, and degaussing, purging or erasing electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1. IBC must make a request to Relocation Management Worldwide to remove data from VEN, after verifying records exist in either ECS or FBMS. The narrative contained in the current MOA, page 15, section 14, reads "All shipment records created during this agreement, all records submitted for uploading into the web application prior to this agreement to establish a historic database resource, and all records completed after this agreement has been terminated and during the agreement closeout period, are the property of IBC and shall be provided to IBC in a downloadable format suitable for maintaining data integrity and viability compatible with effective data management protocols. IBC may request record updates for incomplete records for up to one (1) year after the MOA termination date."

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.

VEN is an online web-based paperless solution to complete PCS moves, track, manage, and report on the relocation programs for IBC's internal and external Federal agency customers. There are risks to the privacy of Federal employees and their family members since the PII is contained in the RMW vendor system, which is accessed through its public facing website. However, only authorized users can access the VEN system. The PII of the Federal employees are collected when they apply for relocation assistance. The respective risks are identified and mitigated by a combination of administrative, physical, and technical controls. The risk for collection of PII is that the system uploads certain forms with some existing fields of PII that the system is not specifically designed to

collect. Although the Travel Voucher has a field for SSN, this information is not required by the relocation process. The SSN field is wiped out before the document is sent out to anyone or uploaded. SSNs are no longer used as a vendor code to assign to any DOI employee for the purpose of identifying the relocating employee. The employee's name and address are entered into the VEN system except for the SSN. Any PII information shown on the vouchers are secure in that only authorized PCS employees have access to the files. Vouchers are submitted via VEN, secure e-mail, and regular postal services to the IBC. Email submissions are protected within the secure DOI network and e-mail system. However, there is a risk that employee emails from personal email accounts containing sensitive information submitted to IBC may not be secured. Sealed mail is delivered to IBC PCS where the mail is opened, date stamped and assigned to the Accounting Technician. The fax machine that can receive the relocation documents is located within IBC PCS department used exclusively by the PCS employees. The FBMS Customer Request Form with Federal employee bank account information will not be uploaded into the VEN system, nor will the bank account information be entered into the VEN system. The form is emailed to the Federal agency customer representative to retrieve Vendor Code from FBMS. The risk of faxing documents is very low as the fax machine is in the IBC PCS section and the recipients of the faxed documents are also in a secured location in their building. Recipients of the faxes either call or e-mail to confirm receipt of the documents. Effective October of 2015 the TA is generated from the FBMS system and it automatically assigns a number to the document. The TA numbers in the past that have shown the employee last name were for the user of the DOI Office of the Secretary (OS) only and not any of the other agencies. This practice of naming the TA document using the employee last name is no longer utilized.

The risks associated with the sharing or disclosure of information is minimized by the administrative, physical and technical controls that are properly defined and enforced are commensurate with the privacy risk level of this system. The VEN application and servers are a dedicated firewall and cloud-based server hosted with Project Host. Employee and PCS staff user role determines the type of access granted. Only authorized PCS employees and staff can access the data in VEN as long as their assigned role allows. All PCS staff employees who have access to the VEN system are trained on the use of the system by one of Lead Certifying Officials before using the system. Verification of role changes is monitored by the Supervisor of the PCS section. Changes would only be necessary if an employee left the PCS section or if their role changed within the section. The PCS Supervisor would notify RMW of the change by submitting and RMW system access form 1. All DOI employees and contractors are required to take privacy and security risk training on an annual basis. VEN is rated as a Federal Information Security Modernization Act (FISMA) moderate system based upon the type of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system. A security plan was completed to address security controls and safeguards for the VEN system. IBC PCS building facilities are monitored and staffed with security personnel, and entry cards and

passwords are utilized for entry. Fax and copier equipment are used by authorized personnel only and cannot be accessed by anyone without the proper Personal Identification Verification (PIV) cards. Employees of IBC use a PIV card to enter the building as well as card entry onto the floor. Access to each floor is limited to only those employees who have the proper clearance for the FMD. In regards to the risks related to records retention and disposition, the system owner of IBC PCS will ensure that the identified records retention and disposition schedule and procedures are strictly followed by all the parties involved and any actions taken in this regard are approved, well-documented and monitored. ARMT/RMW/CRS, as the joint party, is obligated to maintain, safeguard, and preserve the records of IBC PCS according to the requirements set forth in the aforementioned MOA and the Data Management Protocol specified by the MOA.

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:

The use of the data collected is relevant and necessary to provide the Federal government's PCS programs with a transportation, delivery and relocation solutions service. FMD uses VEN as an online web-based paperless solution to complete PCS moves, and track, manage and report on the relocation programs for IBC's internal and external Federal agency customers.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Coordinators and/or Accounting Technicians will review entries for accuracy using the information provided by the relocating employees and the agency approving officials.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ Yes, processes are being consolidated.

☒ 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:

IBC Coordinators and/or Accounting Technicians will have access to VEN. RMW is responsible for troubleshooting issues and updating relocation rates.

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

Access to the system is via SSO or by entering a username and password (If no PIV card) and is also limited to user roles. User roles are submitted to RMW via the RMW System Access Form 1 by the IBC PCS Supervisor to set security parameters before any user is allowed access.

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.

Privacy Act contract clauses were included in the contract. The VEN system is hosted by Project Host through a service level agreement with RMW which outlines the infrastructure and platform maintenance, monitoring and support. Project Host and RMW have limited access for troubleshooting purposes, and do not have access to the VEN records.

☐ 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.

☒ No

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

☒ Yes.

All database tables have fields that allow for reporting and audit transactions. The change log tracks the user and records before and after value changes on the order form. User authentication logs are generated when the user accesses the system.

☐ No

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

The username, Logon Date, Failed Attempts are collected as a function of monitoring the individuals.

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

Each employee authorized to access the VEN system will be credentialed via a PIV card by the RMW Administrator which allows them to either view only certain screens or add or make changes depending on their roles. IBC PCS Coordinators can only add and make

changes on entry screens. The access and role information are only visible to System Administrator Role.

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.

(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.

(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.

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 IBC Financial Management Directorate, Deputy Associate Director serves as the VEN Information System Owner and the official responsible for oversight and management of the VEN security and privacy controls and the protection of the information processed and stored by the VEN system. The Information System Owner and Information System Security Officer 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 within the system, in consultation with DOI Privacy Officials.

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 VEN Information System Owner is responsible for oversight and management of the VEN security and privacy controls, and for ensuring to the greatest possible extent that IBC PCS data is properly managed and that all access to the data has been granted in a secure and auditable manner. The Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of the PII is reported to DOI-CIRC, the DOI incident reporting portal in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the Departmental Privacy Officer.