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: Electronic Enterprise Forms System (eEFS)
Bureau/Office: Office of the Chief Information Officer
Date: December 20, 2016
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: Teri_Barnett@ios.doi.gov
Phone: (202) 208-1605
Address Line: 1849 C Street, NW, Mail Stop 5547 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: *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 Electronic Enterprise Forms System (eEFS) is a component of the eMail Electronic Records and Document Management System (eERDMS) program for the Department of Interior (DOI). It is an application program that supports the consolidation and automation of existing

Departmental paper-based and non-automated forms. These forms are converted into an electronic format and managed in eEFS by the Departmental Forms Manager within the Office of the Chief Information Officer (OCIO). The eEFS is available to DOI employees on an internal portal where Departmental and bureau/office forms are posted.

The eEFS will increase efficiency and responsiveness through the centralization and automation of all DOI forms, and allow DOI leadership to monitor and manage business trends resulting from forms processing. In addition, DOI will be able to modernize many of the manual static processes being used by implementing forms with workflow, leveraging digital and electronic signatures and enabling the utilization of real-time workflow process.

C. What is the legal authority?

5 U.S.C. 301, Departmental Regulations; 43 U.S.C. 1451, the Department of the Interior, Establishment; 44 U.S.C. Chapter 35, Paperwork Reduction Act; 40 U.S.C. 140, 40 U.S.C. § 11101-11703, Clinger-Cohen Act; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, Streamlining Service Delivery and Improving Customer Service; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments"; and Presidential Memorandum, "Building a 21st Century Digital Government".

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*

010-000001739; eMail Electronic Records and Document Management System (eERDMS) System Security Plan.

☐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	No	

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

The DOI Office of the Solicitor has determined that this is not a Privacy Act system of records, and therefore a Privacy Act system of records notice is not required to be published in the *Federal Register*. There are forms that collect personal information from individuals that may be covered under published government-wide, Department-wide, Bureau, or Office Privacy Act system of records notices. Individuals must review the applicable system of records notice for each form submitted for specific information pertinent to the collection and maintenance of information. DOI Privacy Act system of records notices may be viewed at https://www.doi.gov/privacy/sorn.

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

☐Yes: *Describe*
☒No

Section 2. Summary of System Data

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

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

☒Financial Information
☒Medical Information
☒Disability Information
☒Credit Card Number
☐Law Enforcement
☒Education Information
☒Emergency Contact
☒Driver's License
☒Race/Ethnicity
☒Social Security Number (SSN)
☒Personal Cell Telephone Number
☒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.*

This is a Department-wide forms system that may contain large amounts of information including, but not limited to: name, username, Social Security number, email address, home or work address, phone number, other contact information, gender, age, date of birth, nationality, country of origin, country of citizenship, citizenship status, passport number, driver's license information, emergency contacts, Tribal enrollment number, Indian tribal information, Federal, state or local government agency identification number, vehicle registration information, information about personal characteristics such as height, weight, race, employment status, employment background and related information, eligibility determinations, Internet Protocol (IP) address, credit card number, bank account information, other financial information, medical information, information concerning disabilities, criminal background information, security clearance, education information, and information regarding certifications and licenses. The system may also include other categories of information obtained from official forms submitted to and processed by DOI.

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

☒Individual
☐Federal agency
☐Tribal agency
☐Local agency
☒DOI records
☐Third party source
☐State agency

☒Other: *Describe*

Information is collected from DOI employees, contractors and volunteers who submit forms to program officials or through the eEFS.

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

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

Information will be collected using forms in the eEFS from DOI employees, contractors, and volunteers. The eEFS currently uses Security Assertion Markup Language to look up and auto fill contact information for Federal employees but does not interface or share information with other systems at this time. DOI anticipates future uses of the eEFS to interact with other internal or external systems to facilitate the business management process, and will update this PIA at that time.

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

PII provided in the Departmental and bureau/office official forms is used by offices or programs to provide a service, process requests, meet legal or policy requirements, or support mission or business needs. Employee PII is collected when users enter the eEFS Portal for the purpose of authenticating the end user through the Active Directory Federated System (ADFS), DOI's logical security access system.

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.*

Individuals submitting forms will have access only to the forms and data they submit. PII contained in the forms is managed by the responsible program office and will be shared with authorized staff for administrative purposes. User PII will be shared to validate or cross-pollinate data as necessary to perform functions of the system. The eEFS is managed by the Departmental Forms Manager within the OCIO who oversees and directs the conversion of the forms, including the setup of the form and various data entry controls, along with parameters for data expiration.

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

PII contained in forms submitted by bureau/office personnel may be shared with the appropriate form owner. The responsible form owner or program official is responsible for ensure any sharing is authorized and complies with policy. Bureau or office forms are added to the eEFS and centrally managed by the Departmental Forms Manager, and bureau/office use of the eEFS is supported by the Bureau/Office Forms Manager. After a form is added to the eEFS, the assigned form owner within the bureau/office will monitor form submissions, including reviewing data and correcting submissions or contacting individuals that submitted the form for additional information or to correct erroneous information, as necessary.

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

PII contained in forms may be shared with officials, employees, or representatives from other Federal agencies who partner or engage with DOI regarding specific program initiatives or activities. The data provided will vary based on the subject matter of the form. Some data pertaining to individuals may be included in these submissions, such as personal information included on incident reports involving accidents or crimes on DOI lands that involve response efforts from numerous Federal agencies.

☐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.*

DOI contractors providing support for the eEFS and the bureau/office forms program will have access to PII submitted through eEFS.

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

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.*

Individuals can consent to or decline the collection of personal information at the point where an individual submits a form. Opportunity to consent or decline varies with each form contained in the eEFS. Pursuant to the Privacy Act and Departmental policy, any form that collects PII that is maintained in a system of records must include a Privacy Act Statement advising individuals of the authority for the information being collected, the purpose and uses of the information, any impact to the individual for not providing the requested information. Certain form fields may be optional, while other form fields are mandatory, and the submission of a form is a voluntary act by the submitter. The impact to the individual for not

completing a form varies with each form, and in some cases failure to complete a form may hinder requests for DOI services.

☐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.*

Form Owners are responsible for working with their Associate Privacy Officers to develop and provide a Privacy Act Statement or Privacy Notice on forms, as necessary and required by law and policy.

☒Privacy Notice: *Describe each applicable format.*

Some forms may contain a Privacy Notice for collections of information that may not be maintained in a Privacy Act system of record, but may have privacy implications. Some forms that collect information for Privacy Act systems also are covered by published SORNs that provide information to the public on information handling practices.

☐Other: *Describe each applicable format.*

☐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 in the eEFS by the Departmental Forms Manager, Form Owners or System Administrators using any word or part of a word or number (a keyword search) such as the form reference number, including personal identifiers or parts of personal identifiers, such as names, Social Security numbers, email addresses, home or work addresses, usernames. Individuals who have submitted forms can only access their data in the eEFS Portal.

I. Will reports be produced on individuals?

☐Yes: *What will be the use of these reports? Who will have access to them?*
☒No

Section 3. Attributes of System Data

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

Individuals submitting forms to DOI will be responsible for the accuracy of the data provided. In addition, each Bureau/Office Form Manager will design their form in a manner that encourages the submission of accurate information. The design process will include process diagramming, including the creation of swim lane process maps. Among other benefits, these process maps will limit data entry options as a user moves through a form to ensure consistency with data entered in earlier fields on the form. Forms will include data integrity validation controls where appropriate, such as drop down menus, check boxes, text field size limitations, and predefined numeric formats. In addition, the system may apply ADFS query validations to autofill contact information for DOI employees using the system.

Form submissions will be reviewed by the responsible Form Owner, who will be notified upon each new form submission. The Form Owner will have the opportunity to review the form and either correct inaccurate data or contact the submitter of the form to request corrections. The system contains an audit function that allows system administrators to check forms review status by running reports on specific Form Owners, and escalating reviews as necessary.

B. How will data be checked for completeness?

Individuals submitting forms to DOI will be responsible for the completeness of the data provided. In addition, each Form Manager will design their form in a manner that enforces the submission of complete information.

After being notified upon each new form submission, the Form Owner will have the opportunity to review the form and either correct inaccurate data or contact the submitter of the form to request corrections or additional information. The system contains an audit function that allows system administrators to check forms review status by running reports on specific Form Owners, and escalating reviews as necessary.

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

By default, data will have a life cycle of twelve months. Form Managers can shorten or lengthen the data life cycle, based upon the nature of the data at issue, retention schedules, or other factors. When data reaches expiration, the Form Owner will receive notification, and will have the option to allow the data to expire or can contact the submitter to request updated information.

The use of ADFS queries will result in automatic updates of DOI employee contact information in eEFS when the contact information is updated in the DOI Enterprise Active Directory, thereby maintaining currency of the information.

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

Retention periods vary depending on the program area for each form. Records contained within the eEFS are retained and disposed of in accordance with applicable Departmental and bureau/office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record or form based on the subject or function and records series.

Master copies of blank forms are maintained under the Departmental Records Schedule (DRS) 1.1B Long-term Administration Records (DAA-0048-2013-0001-0002), which has been approved by NARA. DRS 1.1B covers records related to administrative management activities including form files with one record copy of each form created by an office with related instructions and documentation. The disposition for these records is temporary and the records are cut-off when the form is discontinued, superseded, or canceled. Records are destroyed three years after cut-off.

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

Records are disposed of in accordance with the applicable Departmental and bureau/office records retention schedules and Department policy for each form based on the program area and agency needs. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with NARA guidelines and 384 Departmental Manual 1.

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

There are risks to the privacy of individuals due to the sensitive PII contained in the forms to support program activities and meet agency mission. As a central repository for all forms, eEFS may collect and store a significant amount of sensitive PII for forms submitted by employees. These risks are mitigated through a series of technical, administrative, and physical controls.

The eEFS has been designed to comply with several important standards in order to ensure consistency, information operability, and precision of data description. In compliance with standards, eEFS utilizes the World Wide Web Consortium Extensible Markup Language (XML), which provides a means for consistent and common data naming conventions. Additionally, eEFS is National Information Exchange Model (NIEM) compliant. NIEM is an XML-based information exchange framework that was designed collaboratively by the Department of Justice and the Department of Homeland Security to develop, disseminate, and support enterprise-wide information exchange standards and processes. The use of these standards in the eEFS will improve development and facilitate a more organized collection of data, reduce the total amount

of data including sensitive PII that the system collects, as well as promote proper data protection, maintenance, and retention practices. eEFS has column level encryption which provides maximum security for personal information, in compliance with FedRAMP requirements. Forms submitted are stored in the eEFS database and forwarded to the Form Owner for processing. eEFS may generate an email notification to appropriate individuals; however, only sender name and form information such as form title and form reference number is included in the email. The form and related records will be archived in eERDMS.

The eEFS is hosted by a Federal Information Security Modernization Act (FISMA) moderate compliant cloud services vendor. The evaluation of cloud-based hosting services is mandatory and the cloud provider complies with all National Institute of Standards and Technology (NIST) standards.

The eEFS consolidates the collection, storage and management of all Departmental and bureau/office forms into a single forms repository. Although data in the eEFS is stored in a common database, the data is separated by limiting access to authorized Form Owners who will have access only to the data contained on the forms they manage. Moreover, the use of a single system will permit all form data collected by DOI to be held and maintained with consistent security, privacy, and records management standards and practices.

The eEFS server is maintained at a central location, which will be mirrored in a secondary location for backup purposes or to provide coverage in the event of a significant outage of the primary system. Absent a significant outage, all data transfers will be unidirectional from the primary server to the backup server. No additional data collection will occur on the backup server. As a result, the data in each location will be consistent. In the event that the backup server is used to run the system during an extended outage period, specific automated controls are in place to ensure the complete transfer of all collected data back to the primary server.

System access is granted to authorized personnel on a need to know basis. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. Different levels of access is dependant on the role of the user. For example, Form Managers may only view submitted forms while end users may access only information they submitted in a form. In some instances, DOl employees acting within the scope of their job duties may submit personal information in standard forms on behalf of another individual such as for human resource purposes.

In addition, firewalls and network security configurations are built into the architecture of the system and fully implemented in accordance with NIST guidelines and Departmental policies. System administrators will monitor user activities to ensure the system is properly used. The eEFS has multiple layers of security that protect content at the object level and can be applied to a user, group of users, or set as a general feature. Account access within the eEFS is also limited to defined time periods. For example, users will be logged out of the system after a period of inactivity. The eEFS can generate both usage and access reports that can be monitored by system administrators.

Additionally, the eEFS contains a user traceability program that can detect unauthorized access attempts or access to files outside of their permissions. DOI employees and contractors are required to complete security, privacy, and records management training, and DOI personnel authorized to manage, use, or operate the system are required to take additional role-based training and sign DOI Rules of Behavior. The audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records management training requirement prevent unauthorized access to data, browsing and misuse.

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 eEFS consolidates existing Departmental and bureau/office forms into a centralized forms program, to increase efficiency, responsiveness and automation of forms. The processing of each form requires the collection and use of specific data in accordance with agency mission. For all forms added to the eEFS, the individual Form Manager is responsible for limiting information collection in accordance with all applicable laws, regulations, and DOI policies, and for ensuring that the data collected is both relevant and necessary.

☐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?

N/A. The eEFS is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

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.*

The eEFS will centralize and consolidate the storage and management of all DOI Departmental and bureau/office forms into a single forms repository. While all of the data in the EFS will be stored in a common database, Form Owners can only access data from the forms they manage.

System access is granted to authorized personnel on a need-to-know basis. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. All personnel must consent to the DOI Rules of Behavior and complete annual security, privacy, and records management training. End users will only have access to the information submitted in their form.

☐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*

DOI Form Managers, system administrators, and authorized users will have access to the data in eEFS. Access to information will be limited to those personnel that have a need-to-know to perform their official duties. Individuals who submit forms will have access only to the forms and data they submit. Form Managers will have access only to the data obtained through the forms they manage. Access to the eEFS by system administrators, authorized program personnel, and contractors is based on least privileges.

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

Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view. Form Manager access to the data is limited to those who have official forms management responsibilities. Access is further governed by DOI IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to assure the integrity and protection of any personal information.

Each form has a designated Form Manager that has access to all information submitted via the form they manage. System administrators have access to audit reports on various aspects of the system's operating controls, including system functions and user actions. Additionally, individuals that submit forms will have access only to their own data.

Computer records are protected by a password system that is compliant with NIST standards as specified in NIST Special Publication (SP) 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations", and NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems". The records contained in this system are safeguarded in accordance with applicable security rules and policies. Access to servers containing records in this system is limited to authorized personnel who have a need to know the information for the performance of their official duties and requires a valid username and password. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels.

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?*

Contractors are involved in the design and development of the system and Privacy Act clauses were inserted in the contracts.

☐No

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

☐Yes. *Explanation*
☒No

K. Will this system provide the capability to identify, locate and monitor individuals?
☐Yes. *Explanation*
☒No

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

The system is not intended to monitor individuals; however, the system will have the ability to audit the usage activity in the system, including the use by system administrators, Departmental Forms Manager, Bureau/Office Form Managers, and Form Owners. Audit information includes reviewable data such as login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new forms by Form Owners. In the event that review of system workflows reveals that reviews are not being performed in a timely fashion, the matter will be escalated.

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

The system is not intended to monitor individuals. However, audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control for unauthorized monitoring. Firewalls and network security configurations are also built into the architecture of the system and NIST guidelines and Departmental policies are fully implemented. System administrators will review the use of the eEFS and the activities of users to ensure that the system is not improperly used, and to prevent unauthorized monitoring or access.

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 eEFS Information System Owner is responsible for the oversight and management of security controls and the protection of agency information processed and stored in eEFS. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in eEFS, in consultation with the Departmental 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 eEFS Information System Owner is responsible for daily operational oversight and management of the system'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 eEFS 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, 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 consultation with the Departmental Privacy Officer.