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: Imaging, Coding and Digitization System (ICDS) Decommissioning
Bureau/Office: Bureau of Trust Funds Administration
Date: September 30, 2022
Point of Contact
Name: Veronica Herkshan
Title: Associate Privacy Officer
Email: BTFA_Privacy@btfa.gov
Phone: (505) 816-1645
Address: 4400 Masthead St. NE, Albuquerque, New Mexico 87109

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 Bureau of Trust Funds Administration (BTFA), formerly, the Office of the Special Trustee for American Indians (OST), Office of Historical Trust Accounting (OHTA) used the Imaging, Coding and Digitization System (ICDS) to convert paper historical DOI records into an electronic format and then added coding to the electronic images, so that they could be searched

in support of the historical accounting of Individual Indian Money (IIM) accounts and ongoing tribal litigation efforts. ICDS consisted of copies of inactive records (no original records) that met their retention period, from the Bureau of Indian Affairs (BIA) and BTFA that were sent to and located at the American Indian Records Repository (AIRR), Federal Records Center (FRC) in Lenexa, Kansas, which were loaded into ICDS to be imaged and coded. The use of the images by users and researchers did not take place within ICDS. ICDS was only used for the processing and coding of the images (DOI record copies), which were then extracted from ICDS and uploaded to another BTFA-OHTA system for viewing and searching. ICDS maintained a copy of the data (coding) and images that resulted from the conversion. Those records contained information that was considered sensitive and confidential and were protected under the Privacy Act of 1974.

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. BTFA, as data owners, are responsible for ensuring data was properly migrated, stored, and disposed of in accordance with the applicable records schedule. ICDS databases were taken offline and decommissioned. Data was archived onto backup tapes/disk, original hard drives were removed, paper records and non-records were inventoried for appropriate disposal, extracted image files were copied to an external hard disk using encrypted software and all are stored at the AIRR. A detailed inventory of all data was provided to BTFA in accordance with the National Archives and Records Administration (NARA) and DOI records management policy and guidance. ICDS was maintained in a secure, central data repository holding all historical account data and images, which are copies of DOI records and no new information was collected from individuals.

C. What is the legal authority?

American Indian Trust Fund Management Reform Act of 1994, Pub. L. 103-412, 108 Stat. 4239.

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*

UII: 010-000000703. ICDS System Security and Privacy 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	N/A	No	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)*

INTERIOR/OS-02, Interior, Individual Indian Money (IIM) Trust Funds, 80 FR 1043, January 8, 2015, which may be viewed on the DOI SORN website at https://doi.gov/privacy/sorn.

☐ No

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

☐ Yes: *Describe*

☒ No. The ICDS is no longer in use, is decommissioned, and no longer maintains PII. The ICDS did not collect information and contained copies of inactive DOI historical records.

Section 2. Summary of System Data

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

☒ Other: ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS was removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI historical records and no new information was collected from individuals.

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 ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS was removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI historical records and no new information was collected from individuals.

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 *Describe*
☒ Other: ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS was removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI historical records and no new information was collected from individuals.

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

The PII data collected supports OHTA's mission to plan and direct the historical accounting of IIM and Tribal accounts, reconcile trust accounts, and perform analysis and reconciling of historical collection, distribution, and disbursement of income from IIM accounts, Indian Trust land, and other revenue sources in support of the DOI and the Department of Justice (DOJ) in litigation, which is directly related to the reason for which the system was designed.

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.*

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

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

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

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

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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.*

☒ No: ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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

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

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☒ None

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

I. Will reports be produced on individuals?

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

☒ No

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

Section 3. Attributes of System Data

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable

manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

B. How will data be checked for completeness?

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. Data was archived onto backup tapes/disk, original hard drives were removed, paper records and non-records were inventoried for appropriate disposal, extracted image files were copied to an external hard disk using encrypted software and all are stored at the AIRR. A detailed inventory of all data was provided to BTFA in accordance with the NARA and DOI records management policy and guidance. ICDS was maintained in a secure, central data repository holding all historical account data and images. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals.

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

ICDS was decommissioned and no longer maintains PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable

manner. ICDS databases were taken offline and decommissioned. ICDS maintained copies of inactive DOI records and no new information was collected from individuals. Data was disposed of in accordance with the approved records disposition procedures in compliance with Departmental policy and NARA guidelines, and preserved at the AIRR.

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 was a limited privacy risk for the decommissioning of the ICDS. ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. The data owners are responsible for ensuring data was properly migrated, stored, and disposed of in accordance with the applicable records schedule.

ICDS databases were taken offline and decommissioned. Data was disposed of in accordance with the approved records disposition procedures, and preserved at the AIRR, a secure DOI Facility. ICDS database(s) have not been replaced, data backed up on disks are stored at the AIRR, were transferred to the BTFA receiving systems, and verified by BTFA, as the data owners. The hardware was decommissioned, ICDS data was archived onto backup tapes and disks and stored at AIRR. BTFA provided adequate physical, technical, and administrative controls to protect the data from unauthorized access or disclosure.

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*

☒ No

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

☐ Yes: *Explanation*
☒ No

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

☐ Yes: *Explanation*
☒ No

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

☐ Users

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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?*

☒ No

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned.

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. ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned. There are physical controls in place that protected the data that was transferred or is still being maintained by BTFA.

(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. ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. ICDS databases were taken offline and decommissioned. There are technical controls in place that protected the data that was transferred or is still being maintained by BTFA.

(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. ICDS was decommissioned and is no longer in use to maintain PII. There are administrative controls in place that protected the data that was transferred or is still being maintained by BTFA.

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.

ICDS was decommissioned and is no longer in use to maintain PII. The data associated with ICDS were removed from the private local area network, and are no longer operational. The Director, Office of Business Management is the ICDS Information System Owner (ISO) who is the official responsible for oversight and management of the security and privacy controls of data processed (copies of DOI records) and stored by ICDS. The ISO and Information System Security Officer (ISSO) is also responsible for ensuring adequate safeguards are implemented to protect privacy in compliance with Federal laws and policies for the data (copies of DOI records) retired and disposed of in ICDS, in consultation with BTFA and DOI Privacy Officials. A decommissioning plan was completed for ICDS which outlined and documented the decommissioning activity, tasks, and procedures to ensure the system was decommissioned in a secure and auditable manner. ICDS databases were taken offline and decommissioned. Data was archived onto backup tapes/disk, original hard drives were removed, paper records and non-records were inventoried for appropriate disposal, extracted image files were copied to an external hard disk using encrypted software and all are stored at the AIRR. A detailed inventory of all data was provided to BTFA in accordance with the NARA and DOI records management policy and guidance. ICDS was maintained in a secure, central data repository holding all historical account data and images, which are copies of DOI records and no new information was collected from individuals.

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 ICDS ISO 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 ICDS ISO and ISSO 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 BTFA Associate Privacy Officer.