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: Loan Management System (LMS)
Bureau/Office: Bureau of Indian Affairs (BIA), Office of Indian Energy and Economic Development (IEED), Division of Capital Investment
Date: December 29, 2020
Point of Contact
Name: Richard Gibbs
Title: Associate Privacy Officer
Email: Privacy_Officer@bia.gov
Phone: (505) 563-5023
Address: 1011 Indian School Rd NW, Albuquerque, New Mexico 87104

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 Loan Management System (LMS) is a major application and the central repository for all guaranteed and insured loans managed by the Division of Capital Investment (DCI) within the Office of Indian Energy and Economic Development (IEED), Bureau of Indian Affairs (BIA) to support the Loan Guarantee, Insurance, and Interest Subsidy Program. It is a commercial-off-the-shelf MicroPact Product Suite Platform as a Service (PaaS) and Software as a Service (SaaS) cloud-hosted system. LMS is hosted in the General Dynamics Information Technology (GDIT)

Federal Risk and Authorization Management Program (FedRAMP)-approved cloud operated by MicroPact. GDIT is one of nine DOI approved cloud hosting providers.

LMS is a case management tool. As a management tool, LMS monitors and reports on active and pending guaranteed and insured loans by tracking and recording payments and unpaid balances, and provides easy access to information on payments and unpaid balances, payments made for paying interest subsidy, credits obtained, service loans made, and premiums paid by the lenders. LMS manages information about the borrower, loan approval, loan budget validation, loan collateral, loan collection, and loan disbursement.

The IEED provides high-level support for the Department's goal of serving tribal communities by providing access to energy resources and helping tribes stimulate job creation and economic development. IEED is committed to achieving long-term goals of promoting Indian economic development, increasing tribal business knowledge, increasing jobs and businesses, increasing capital investment, and providing assistance for developing energy and mineral resources. One of the three Divisions that makes up IEED is DCI. DCI manages the Indian Loan Guarantee, Insurance, and Interest Subsidy Program, which helps borrowers secure business financing on commercially reasonable terms.

The purpose of the Loan Guarantee, Insurance, and Interest Subsidy Program is to encourage eligible borrowers to develop viable Indian businesses through conventional lender financing. The direct function of the Program is to help lenders reduce excessive risks on loans they make. That in-turn helps borrower secure conventional financing that might otherwise be unavailable.

C. What is the legal authority?

25 U.S.C. § 1451, as amended by Pub. L. 98-449, Indian Financing Act Amendments of 1984; 25 U.S.C. §§ 1481-1499, Subchapter II: Loan Guaranty and Insurance; and 25 U.S.C. § 1511 *et seq.*, Subchapter III: Interest Subsidies and Administrative Expenses; 25 U.S.C. § 5133; and 25 CFR Part 103, Loan Guaranty, Insurance, and Interest Subsidy

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: 010-000002479, Loan Management System (LMS), 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	Not Applicable	No	Not Applicable

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)*

Records in LMS are maintained under, BIA-13, Loan Management and Accounting System (LOMAS), 73 FR 40595; July 15, 2008, which may be viewed at https://www.doi.gov/privacy/bia_notices. This SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.*

☐ No

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

☒ Yes: *Describe*

OMB Control Number 1076-0020, Loan Guarantee, Insurance, and Interest Subsidy Program (25 CFR 103), Expires June 30, 2022

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Security Clearance
☒ Gender
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Other Names Used
☒ Driver's License
☒ Financial Information
☒ Social Security Number (SSN)
☒ Race/Ethnicity
☒ Spouse Information
☒ Birth Date
☒ Group Affiliation
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: In addition to the PII identified above, the Employee Identification Number (EIN); Tax Identification Number (TIN) for businesses; borrower's court records, death certificate; loan guarantee ID; borrower's banking information; loan guarantee or loan insurance certificate number; the lender's internal loan number; and loan origination, payment and balance activity are contained within the loan application. Social Security numbers (SSN) are used to ensure

accurate identification of loan borrowers and guarantors because people may have the same name and date of birth. Accurate identification is necessary as is providing a SSN to the U.S. Department of Justice and the Department of the Treasury when a loan is referred for enforced debt collections or foreclosure; to administer the Loan Guarantee, Insurance, and Interest Subsidy Program and to comply with legal requirements when attempting to collect program losses, report taxable income, and for cancellation of indebtedness due to collectability.

Username and password are used for authentication purposes.

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*

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: The vast majority of PII is information on borrowers, supplied directly from borrowers to lenders using the lender's own forms and procedures. That information is passed on to DCI in accordance with 25 CFR sections 103.12, 103.13, and 103.14 when the lender deems it appropriate to use the Indian Loan Guarantee, Insurance, and Interest Subsidy Program. Applications may arrive electronically, using a secure Internet connection, or in paper form through the US Postal Service or another delivery service, such as FedEx. When necessary to collect debts or report taxable income as required by law, supplemental information concerning borrowers is acquired through LexisNexis over the Internet, using a secure connection to that service. PII is used to administer the Indian Loan Guarantee, Insurance, and Interest Subsidy Program and to comply with legal requirements to attempt to collect program losses and to report taxable income, such as cancellation of indebtedness due to uncollectability.

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

The primary use of the PII collected and maintained in LMS is to administer the Loan Guarantee, Insurance, and Interest Subsidy Program by tracking and recording payments and unpaid balances and providing information on payments made for paying interest subsidy, credits obtained, service loans made, and premiums paid by lenders. It is also used to determine if the applicant will qualify for a guaranteed loan, insured loan, loan repayment or interest subsidies under the guidelines of the Program. PII is also used to report taxable income, collect program losses, cancel indebtedness due to uncollectability, and comply with legal requirements.

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.*

Office of Financial Management, Loan Accounting Section. The Loan Accounting Section is authorized access to LMS to monitor the status of Guaranteed and residual Direct loans.

Division of Capital Investments. The collected information on borrowers is used to determine if the applicant (the borrower's proposed lender) will qualify for a loan guarantee, loan insurance, or interest subsidies.

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

Data may be shared with the DOI Office of the Solicitor to recover debts owed by borrowers, in the event of default and transfer of the lender's rights in loan documents to DCI pursuant to 25 CFR section 103.38.

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

To the Department of the Treasury and/or U.S. Department of Justice in the form of information on individual delinquent borrowers or borrowers who have misused funds in order to support debt collection efforts.

To Congress in the form of periodic reports on the status of the Indian Affairs Loan Guarantee, Insurance, and Interest Subsidy Program in order to document the use of program funds.

Data is shared and reported to other Federal agencies, including the Department of the Treasury, Office of Management and Budget, and other agencies that perform external monitoring of the Indian Loan Guarantee, Insurance, and Interest Subsidy Program.

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

Borrower information may be shared with State or Local agencies when necessary and compatible with the purpose of the system as authorized under the published routine uses in the BIA-13 SORN, *e.g.*, to record and perfect a lien on collateral.

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

Information may be shared with contractors providing Information Technology support services for routine maintenance, future system enhancements and technical support. PII may be shared with Zone Manager and Loan Accounting Staff contracted administrative assistants to perform official functions in support of the LMS system.

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

Information is shared with credit monitoring and consumer reporting agencies in the form of loan information regarding payment delinquencies. Pursuant to 5 U.S.C. 552a(b)(12), records may be disclosed to consumer reporting agencies as they are defined by the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

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.*

This system contains records on corporations and lending institutions that are not subject to the Privacy Act. The information collected from these corporations and lending institutions is for obtaining a guarantee or insurance on a loan. The information maintained on corporations and business entities is limited to contact information: name, TIN, business address, business telephone number, accrediting information, business credit report, and publicly available information. Individual borrowers and individuals acting on behalf of corporations voluntarily provide their information to lenders, and lenders pass that information on to DCI in the course of applying for program benefits.

Applying for a loan guarantee is voluntary, as is the underlying effort by a borrower to secure a loan from the lender. However, lenders must provide all required information concerning borrowers to qualify for a guarantee on a loan. Response is required to obtain a benefit. Failure to provide necessary information may cause an application to be declined.

☐ 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.*

A Privacy Act Statement is included on the forms provided to borrowers and lenders. The Office of Management and Budget approved these forms as part of the BIA Information Collection 1076-0020, Loan Guarantee, Insurance, and Interest Subsidy Program. The forms associated with this collection allow the BIA to determine the eligibility and creditworthiness for loans and otherwise ensure compliance with program requirements. Each form includes the requisite information on the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment and the published BIA-13, Loan Management and Accounting System (LOMAS), 73 FR 40595; July 15, 2008, which may be viewed at https://www.doi.gov/privacy/bia_notices. The BIA-13, Loan Management and Accounting System (LOMAS) SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-

108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

☒ Other: *Describe each applicable format.*

Users are presented with a DOI security warning banner that informs them they are accessing a DOI system, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

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

LMS generates a system loan guarantee number to initially create a new loan case file, which is the primary method used to retrieve information. Zone Managers and Loan Accounting Staff can retrieve information using the SSN, TIN/EIN, borrower last name, loan guarantee number and banking information. Advanced searches can retrieve any information input in any field of any data entry screen in the system. Users with the proper permissions can create customized result sets containing any information in the system.

I. Will reports be produced on individuals?

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

Guaranteed lenders must report their borrower's loan payment history quarterly so that BIA can recalculate the government's contingency liability per 25 CFR § 103.33. These reports contain the lender's name, borrower's name, the loan guarantee or loan insurance certificate number; the lender's internal loan number; and the date and amount of all loan balance activity for the reporting period.

DCI produces periodic statistical reports on guaranteed and direct loans for its defined zones, capturing information such as the total loan amount, duration of the loan, the loan guarantee percentage, allocated subsidy, subsidy payments, borrower repayment, and outstanding balances to recalculate the government's contingency liability per 25 CFR § 103.33. These reports may include identifying information about both the lender and the borrower of the loan, including the lender's name, borrower's name, the loan guarantee or loan insurance certificate number; the lender's internal loan number; and the date and amount of all loan balance activity for the reporting period.

Loan Accounting Staff produces Treasury Report on Receivables (TROR) and Debt Collection Activity reports for distribution to the Department of Treasury, Office of Management and Budget, DOI Office of the Chief Financial Officer, and other agencies that perform external monitoring of the program. The content of these reports is produced based on the information requested by the monitoring entity. Other reports generated consist of aged receivables, note payment history, transactions over specific periods, and project collections. These reports may include identifying information about the borrower of the loan. These reports include loan numbers and may include borrower names. Most reports will disclose outstanding balances on

the loans (total and/or detailed by principal, interest and fees). Collections and payment history will include payment and/or deposit amounts and dates and may include check numbers and/or Treasury generated deposit numbers.

Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. Audit logs capture account creation, modification, disabling, and termination; logon date and time, number of failed login attempts, files accessed, user actions or changes to records. Audit Logs also collect information on system users such as username. System administrators and the information system owner have access to these activity reports.

☐ No

Section 3. Attributes of System Data

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

Lenders are required to check and verify borrower information for accuracy before submitting a program application per 25 CFR § 103.30(a). DCI Zone Managers review all program applications for completeness and accuracy.

Users are responsible for ensuring the accuracy of the data associated with their user accounts. Data is checked for accuracy during the account creation process.

B. How will data be checked for completeness?

Lenders are required to maintain a complete and current history on all program guaranteed or insured loan transactions per 25 CFR § 103.32. Zone Managers and the DCI representative establishing meetings of DCI's credit committee review loan guarantee/insurance applications for completeness in accordance with 25 CFR sections 103.12 and 103.13. Zone Managers communicate with the lender, and if necessary, the borrower, if a program application appears to be incomplete or inaccurate. Additionally, DCI's credit committee members consider all aspects of program applications, including completeness, when recommending whether to approve or disapprove a program application.

Data is checked for completeness during the account creation process. Users are responsible for ensuring the completeness of the data associated with their user accounts.

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

Lenders are required to check, verify and update borrower information in accordance with 25 CFR sections 103.30 and 103.32. At the time of application, DCI Zone Managers and DCI's credit committee review application materials to make sure borrower data is not outdated or stale beyond, *e.g.*, the 90-day tolerance for credit reports stated in 25 CFR section 103.12(e). Thereafter Lenders are to report loan payment history in accordance with 25 CFR 103.33, and to notify DCI in the event of loan modification, change in borrower identity, or borrower default in accordance with 25 CFR sections 103.34 and 103.35. DCI officials also individually and collectively monitor the subsequent history of most projects begun with a program guarantee or insurance.

User account information is provided directly by the user during account creation and can be updated by the user. Users are responsible for the accuracy of their records.

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

Records related to the Loan Management System are scheduled with the National Archives and Records Administration (NARA) as permanent. These records are maintained according to the Indian Affairs Records Schedule, 4200 records series. NARA approved the disposition authority March 31, 2005, under Job Number N1-075-05-001. Records included in this series are Approved Indian Loan Guarantee files, Disapproved Indian Loan Guaranty Files, and Loan Service Files. Approved Indian Loan Guaranty Files are cut-off at the end of the fiscal year in which the loan is terminated or paid off. The office of record maintains the records for a maximum of 5 years after cut-off; and then transfers them to the American Indian Records Repository (AIRR), which is a Federal Records Center. Disapproved Indian Loan Guarantee Files are cut-off at the end of the fiscal year in which loan disapproval is determined. The office of record maintains the records for a maximum of 5 years after cut-off; and then transfers them to the AIRR. Loan Service Files are cut-off at the end of each fiscal year. The office of record maintains the records for a maximum of 5 years after cut-off; and then transfers them to the AIRR. In accordance with the Indian Affairs Records Schedule, the subsequent legal transfer of records to the National Archives of the United States will be jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

LMS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001-0013), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 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?

Data and information maintained within LMS is retained under the appropriate NARA approved Indian Affairs Records Schedules (IARS). Data disposition follow NARA guidelines and approved Records Schedule for transfer, pre-accession and accession activities to NARA. These activities comply with 36 CFR 1220-1249, specifically 1224 - Records Disposition Programs and Part 1236 - Electronic Records Management, NARA Bulletins and the Bureau of Trust Funds Administration, Office of Trust Records, which provides records management support to include records management policies and procedures, and development of BIA's records retention schedule. System administrators dispose of DOI records by shredding or pulping for paper records, and degaussing or erasing for electronic records 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 is a moderate risk to the privacy of individuals due to the sensitive PII contained in LMS. LMS has undergone a formal Assessment and Authorization and granted an authority to operate (ATO) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. LMS is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53. DCI and BIA implemented administrative, technical and physical controls to mitigate the privacy risks against unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information.

The LMS Project has an Interagency Agency Agreement (IAA) with the Interior Business Center's Division of Acquisition Services for Cloud Hosting Services. Through a contract vehicle with GDIT, MicroPact Inc. hosts LMS. MicroPact is FedRAMP-certified as a cloud service provider that has met all requirements for LMS information categorized as Moderate in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). LMS follows NIST criteria for categorization, selection, development, implementation, assessment, authorization, and monitoring of security controls.

DCI and BIA have entered into an agreement for BIA's use of LMS that includes provisions pertaining to the handling, sharing, and retention of relevant data designed to ensure privacy and data collection. As the managing agency, DCI is responsible for ensuring LMS' management, operational, and technical controls established by NIST SP 800-53 are in place to mitigate the security and privacy risks for Federal agency use of the system. BIA has reviewed the DCI LMS authorization package for issuance of an ATO. BIA has ownership and control of BIA records in LMS and is responsible for ensuring adequate security and privacy controls are implemented to prevent unauthorized access or disclosure.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Access to files is strictly limited to authorized personnel who need access to perform official functions. System and information access are based on the "least privilege" principle combined with a "need-to-know" in order to complete assigned duties. BIA manages LMS user accounts using the Identity Information System (IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of LMS user accounts. System administrators utilize user identification, passwords, and audit logs to ensure appropriate permissions and access levels are enforced to ensure separation of duties is in place. The audit trail includes the identity of each entity accessing the system; time and date of access, and activities performed; and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system is reported to IT Security. Annually employees, complete privacy training which includes the topics of inappropriate use and unauthorized disclosure. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure they have an understanding of their responsibility to protect privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. Physical,

operational, and technical controls are in place and other security mechanism have also been deployed to ensure data and system security such as firewalls, virtual private network, encryption, malware identification, intrusion detection, and periodic verification of system user activity. Audit logs are routinely checked for unauthorized access or system problems. Data is encrypted during transmission and at rest. Hardcopy documents containing PII are secured in a locked office, desk drawer or file cabinets when not in use to control access, protect against inappropriate use or disclosure to unauthorized individuals.

There is a risk that LMS may collect and share more information than necessary to complete program goals and objectives, or information may be used outside the scope of the purpose for which it was collected. Only the minimal amount of information needed to perform official functions for which the system was designed is collected and maintained in order to provide a service or perform official functions. Authorized personnel with access to the system are instructed to collect the minimum amount of information needed to perform official functions for which the system was designed and are to share information only with individuals authorized access to the information and that have a need-to-know in the performance of their official functions. Employees complete privacy training which includes topics on the collection and unauthorized disclosure of information. Users are advised not to share sensitive data with individuals not authorized access and to review applicable system of records notice before sharing information. Employees are aware information may only be disclosed to an external agency or third party if there is informed written consent from the individual who is the subject of the record; if the disclosure is in accordance with a routine use from the published SORN and is compatible with the purpose for which the system was created; or if the disclosure is pursuant to one of the Privacy Act exceptions outlined in 5 U.S.C. 552a(b). Before authorizing and granting system access, users must complete all mandatory security, privacy, records management training and sign the DOI Rules of Behavior to ensure employees with access to sensitive data understand their responsibility to safeguard individual privacy. Employees must acknowledge their understanding and responsibility for protecting PII, complying with privacy requirements under the Privacy Act, E-Government Act of 2002, OMB privacy guidance, and DOI privacy policy. They must also acknowledge their understanding that there are consequences for not protecting PII and failing to meet privacy requirements. System access and restrictions are explicitly granted based on the user roles and permissions in accordance with job descriptions and “need-to-know” factors, based on the “least privilege” principle. Access restrictions to data and various parts of the system’s functionality is role-based and requires supervisory approval. Access controls and system logs are reviewed regularly as part of the continuous monitoring program. LMS meets BIA’s information system security requirements, including operational and risk management policies.

There is a risk of maintaining inaccurate borrower information that could result in unfavorable judicial disposition should DCI ever honor a loan guarantee or insurance claim and thereafter attempt to enforce collection of an unpaid borrower debt. This risk is mitigated through regulatory provisions that require lenders to check borrower information for accuracy before submitting it to DCI, particularly 25 CFR section 103.30(a). In addition, DCI Zone Managers review each loan application for completeness and accuracy before entering the data into LMS, which is itself fully auditable.

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. In regard to information handling and retention procedures, DCI is responsible for managing and disposing of BIA records in LMS as the information owner. Records in this system are related to Indian Trust Assets and have a permanent retention schedule due to their continued business and Tribal value. DCI ensures only records needed to support its program, Tribes, and Tribal members is maintained. DCI maintains the records for a maximum of five years or when no longer needed for current business operations, at which time they are transferred to the American Indian Records Repository, a Federal Record Center for permanent safekeeping in accordance with retention schedules approved by NARA under Job Code N1-075-05-001. LMS system usage records are covered by the Departmental Records Schedule 1.4A, Short Term Information Technology Records, System Maintenance and Use Records (DAA-0048-2013-0001), approved by the National Archives and Records Administration (NARA). These records include system operations reports, login and password files, audit trail records and backup files. The disposition is temporary. Records are cut-off when superseded or obsolete and destroyed no later than 3 years after cut-off. Information collected and stored within LMS is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk that individuals may not have adequate notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and the published BIA-13, Loan Management and Accounting System, 73 FR 40595, July 15, 2008, which may be viewed at https://www.doi.gov/privacy/bia_notices. Lenders are provided a Privacy Act Statement (PAS) during the application process that explains the authority, purpose, and impacts for not providing requested information. When lenders seek a program guarantee or insurance, they must alert borrowers and secure authorization to forward loan application materials for program application purposes, if such authorization is not already provided in the borrower's application to the lender. Program regulations contain an information collection notification at 25 CFR section 103.45. Additionally, PAS are part of the Loan Guarantee, Insurance, and Interest Subsidy Program (24 CFR 103) information collection. The PIA, SORN, and PAS provide a detailed description of system source data elements and how an individual's PII is used.

There is a risk related to external sharing of data with Federal agencies and non-Federal organizations. The BIA-13 SORN covers the collection of this information and describes the routine uses that cover the sharing of data with Federal agencies and non-Federal organizations. BIA restricts the sharing of data for the specific purposes and only to those Federal agencies and non-Federal organizations identified in the published BIA-13 SORN.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. LMS is hosted and administered within a DOI-approved and FedRAMP-certified hosting center. The cloud service provider will implement protections, controls and access restrictions as required to maintain the necessary FedRAMP certification. The data residing in the system is backed up on a nightly basis. BIA manages system access using the Identity Information System

(IIS), a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of system user accounts.

In addition to the risk mitigation actions described above, the BIA maintains an audit trail of activity is maintained sufficiently to reconstruct security relevant events. The BIA follows the "least privilege" security principle, such that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. Access to the DOI Network requires two-factor authentication. Users are granted authorized access to perform their official duties and such privileges comply with the principles of separation of duties. Controls over information privacy and security are compliant with NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. DOI employees must take Information Management Training (IMT) which includes Cybersecurity (FISSA), Privacy, Records Management, and Controlled Unclassified Information before being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. DOI personnel also sign the DOI Rules of Behavior. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The data used in LMS is both relevant and necessary to the purpose for which the system was designed. The information (data) stored on this system is directly relevant and necessary to accomplish the DCI and Loan Accounting mission to helps borrowers secure business financing on commercially reasonable terms.

☐ No

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

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

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

☐ Yes: *Explanation*
☒ No

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

☐ Yes: *Explanation*
☒ No

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

Not Applicable. LMS 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.*

☐ 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*

Access to the data in LMS is limited to Federal employees and contractor support staff within DCI. The specific users are Zone Managers and their assistants (who are contractors), Loan Accounting Staff (Federal users and contractors), Collection Coordinator, and Financial Reporting Officers. All of the above-mentioned employees, including the IT contractors require access to the system and the data in order to carry out their official functions.

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

Users are only given access to data on a 'least privilege' principle and 'need-to-know' to perform official functions. BIA manages LMS user accounts using IIS, a self-contained system that provides workflow and access controls, which includes establishing, activating, modifying, reviewing, disabling and removal of LMS user accounts. Federal employee access requires supervisor approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner.

LMS has advanced security features to control and restrict access to audits and associated artifacts based on assigned group membership or level of authority and maintains detailed audit log of all user activity, ensuring compliance with role-based access, segregation of duties, and least privilege principle, such that only the least amount of access is given to a user to complete their required duties.

Additionally, the system maintains audit logs, as required by BIA specific audit requirements, capturing a variety of user actions such as successful and unsuccessful user logins and

modifications made by different users along with date and time stamps. System administrator can monitor user activities via audit logs.

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 required to sign nondisclosure agreements as a contingent part of their employment. They are also required to sign the DOI Rules of Behavior and complete security and privacy training before being granted access to a DOI computer system or network. Information security and role-based privacy training must be completed on an annual basis as a contractual employment requirement. The following Privacy Act contract clauses were included in the contract.

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.224-3, Privacy Act Training (Jan 2017)
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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*

The purpose of LMS is not to monitor individuals, however user actions and use of the system is monitored to meet DOI security policies. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. LMS has advanced security features to control and restrict access to audits and associated artifacts based on assigned group membership or level of authority and maintains detailed audit log of all user activity, ensuring compliance with role-based access, segregation of duties, and least privilege principle.

☐ No

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

The LMS system is not intended to monitor individuals; however, the system has the functionality to audit user activity. Audit logs can be used to run reports detailing an individual user's authorized access and actions performed within the system. The logs capture account creation, modification, disabling, and termination. Additionally, the system may capture a variety of user actions and information such as usernames, logon date, number of successful and unsuccessful logins, and modifications made to data by different users along with date and time stamps. Firewalls and network security configurations are also built into the architecture of the system and NIST Special Publication 800-53, Security and Privacy Controls for Federal

Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring.

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

LMS has the ability to audit the usage activity in the system. Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. LMS System Administrators review the use of the system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized use or access. LMS assigns roles based on the principles of 'least privilege' and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users will be required to consent to DOI Rules of Behavior. Users must complete annual Information Management and Technology (IMT) Awareness Training, which includes Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially upon employment and annually thereafter, to ensure an understanding of their responsibility to protect privacy.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy to ensure systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The LMS audit trail will include system user's username, logon date and time, number of failed login attempts, files accessed, and user actions or changes to records. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system is reported immediately to IT Security.

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 Associate Chief Information Officer is the Information System Owner for LMS. The Information System Owner (ISO), Information System Security Officer (ISSO), and authorized bureau/office system managers 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 LMS. The ISO and the Privacy Act system managers are responsible for addressing any Privacy Act complaints and requests for notification, access, redress, or amendment of records in consultation with the 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 LMS ISO and ISSO are responsible for the central oversight and management of the LMS 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 LMS ISO, ISSO, and bureau and office system administrators 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 DOI Privacy Officials. Program officials and users are also responsible for protecting PII and meeting requirements under the Privacy Act and Federal law and policy, and for reporting any potential compromise to DOI-CIRC and privacy officials.