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: Financial Assistance and Social Services – Case Management System Cloud (FASS-CMS Cloud)
Bureau/Office: Bureau of Indian Affairs/Office of Indian Services
Date: October 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 Bureau of Indian Affairs (BIA) Office of Indian Services' (OIS) mission is to facilitate support for tribal people and tribal governments by promoting safety, quality living environments, strong communities, and self-sufficiency and individual rights, while enhancing protection of the lives, prosperity, and wellbeing of American Indians and Alaska Natives. Under this mission area and the Department of the Interior (DOI) strategic goal of Serving Communities, the OIS, Division of Human Services developed the Financial Assistance and

Social Service (FASS) program to promote the safety and the well-being of Indian communities and individual Indians.

FASS-CMS Cloud is a commercial, off-the-shelf (COTS) major application provided as Software-as-a-Service (SaaS) housed in the Microsoft Government Community Cloud (GCC). FASS-CMS Cloud was designed to improve social service case worker productivity and decision-making by providing more complete case information and conforming to the case worker's workflow, while enabling better resource management. The FASS-CMS Cloud automates the application process, ensuring compliance with eligibility criteria; automates case workflow, provides case tracking and records management, supports financial payments for eligible Indian clientele, and provides management with reports for performance and compliance management. It is a comprehensive social services case management system for the BIA.

The primary purpose of FASS-CMS Cloud is to:

- Help the Division of Human Services' social service workers, management and Tribal members determine eligibility of individuals applying for or receiving financial assistance and/or social services, to support financial assistance and social service payments to eligible clients;
- Provide individual records on social services and direct assistance to individual Indians;
- Provide management with an automated information system for program planning, management utilization, and adequate reporting for performance and compliance management;
- Improve the case worker's productivity and decision-making by providing more complete case information, while enabling better resource management;
- Automate the application process and case workflow to ensure compliance with eligibility criteria;
- Provide adequate tracking and recordkeeping;
- And, to support the financial payments to eligible Indian clientele.

C. What is the legal authority?

25 U.S.C. 13d (1-3), *the Snyder Act of 1924* (Pub. L. 67-95); 25 CFR Part 20, Financial Assistance and Social Services Program; 25 CFR Part 23, Indian Child Welfare Act; 25 CFR Part 115, Trust Funds for Tribes and Individual Indians; 25 CFR Part 63, Indian Child Protection and Family Violence Prevention Act (Pub. L. 101-630); Native American Children's Safety Act. (Pub. L. 114-165); Indian Employment, Training and Related Services Consolidation Act of 2017 (Pub. L. 115-93); Indian Self-Determination and Education Assistance Act of 1975 (Pub. L. 93-638), as amended; Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Pub. L. 104-193), Indian Alcohol and Substance Abuse Prevention and Treatment Act of 1986 (Pub. L. 99-570).

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 Code: 010-000000020, Financial Assistance and Social Services – Case Management System (FASS-CMS Cloud), 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	Not Applicable	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 FASS-CMS Cloud are maintained under DOI system of records notice BIA-08, Financial Assistance and Social Services – Case Management System, 76 FR 56787; September 14, 2011, which may be viewed at https://www.doi.gov/privacy/bia_notices. Vendor record creation and payment data are maintained under DOI system of records notice: DOI-86, Accounts Receivable: FBMS, 73 FR 43772; July, 28, 2008, which may be viewed at: https://www.doi.gov/privacy/doi-notices. The BIA-08 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 1076-0017, Financial Assistance and Social Services Program, 25 CFR 20; Expires October 31, 2020

OMB Control Number 1076-0131, Indian Child Welfare Quarterly and Annual Report, Expires April 30, 2021

A New Information Collection is proceeding through the OMB clearance process. It is titled, Supervised Individual Indian Money Accounts, Notice of Information Collection, 84 FR 71453, 71453-71454, published on 12/27/2019, which can be seen at Federal Register-Agency Information Collection Activities; Supervised Individual Indian Money Accounts.

☐ No

Section 2. Summary of System Data

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

☒ Name	☒ Social Security Number (SSN)	☒ Birth Date
☒ Gender	☒ Race/Ethnicity	☒ Spouse Information
☒ Financial Information	☒ Personal Cell Telephone Number	☒ Marital Status
☒ Group Affiliation	☒ Tribal or Other ID Number	☒ Medical Information
☒ Personal Email Address	☒ Home Telephone Number	☒ Disability Information
☒ Biometrics	☒ Other Names Used	☒ Law Enforcement
☒ Emergency Contact	☒ Child or Dependent Information	☒ Driver's License
☒ Education Information	☒ Employment Information	☒ Military Status/Service
☒ Mailing/Home Address	☒ Other: Tax Identification Number (TIN), legal proceeding documents related to Social Services cases (i.e. Court Orders, Court Petitions, Court Reports, Guardianship Orders, Power of Attorney) and Individual Indian Monies Account information.	

The solicitation of the Social Security Number (SSN) is authorized by 25 CFR § 20.404 and §20.506, and Executive Order 9397, as amended by EO 13478, to meet social services requirements. The SSN is a required identifier in the social services assessment (25 CFR § 20.404), the foster care case file (25 CFR §20.506). TINs and SSNs are also collected to create a Financial Business Management System (FBMS) Vendor Record for the purposes of making financial assistance and social services payments to vendors. FBMS uses it to assign a unique identifier for the individual or third party vendor to ensure payments are correctly recorded and disbursed.

FASS-CMS Cloud also contains records concerning a number of third party vendors, including, residential care facilities, group homes, and funeral homes that are not subject to the Privacy Act, as well as data on a small proportion of sole proprietors, which is covered by the Privacy Act, for example foster care homes. Records pertaining to individuals applying for services on behalf of a social services client or eligible individual may include the individuals or third party vendor's personal information. PII collected from these individuals includes phone numbers, email addresses, physical address, and other contact information, Tax Identification Number, SSN, financial institute/ bank account number, amount paid, license number, issuing agency, and other information related to services provided as a third party vendor. For example, information collected for a foster care placement may also include PII information on each household member residing in the home as listed above and in Section 2(A).

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: *Describe*

FASS-CMS Cloud and the FBMS interface via an encrypted, manual secure file transfer protocol. FASS-CMS Cloud creates new/updates contact and vendor records and the approval/authorization of payments, generates transmission of the record to FBMS. FBMS then responds with a file which contains FBMS new vendor identifiers, confirmation information to update vendor information, and the rejection of payment information to FASS-CMS Cloud.

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

The intended use of the PII collected is:

- To assist social service workers determining an applicant's eligibility for financial assistance and social services provided by the BIA;
- To support financial assistance and social service payments to eligible clients;
- To provide individual records on social services and direct assistance to individual Indians;
- And, in conjunction with the client, to complete an individual self-sufficiency plan, which spells out the details necessary for a person to assume a meaningful job and must indicate the services received will meet the individual's and Tribal goals.

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.*

Information may be shared with BIA employees acting in their official capacity in the performance of official functions to assist in the determination of an applicant's eligibility for financial assistance and social services provided by the BIA; and, in conjunction with the client, to complete an individual self-sufficiency plan, which spells out the details necessary for a person to assume a meaningful job and must indicate the services received will meet the individual's and Tribal goals.

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

Information may be shared with Bureau of Trust Funds Administration for the purpose of managing supervised Individual Indian Monies (IIM) accounts including restricting and unrestricting accounts and disbursing funds from IIM accounts. This includes Distribution Plans which may include the Name, DOB, Social Security Number, IIM Account Number, Address, and Bank Account Information, Payee Name and Address. This also includes restriction letters such as the Kennerly letter (notification that must be provided to the account holder that a decision has been made by the Officer-in-Charge to supervise the IIM account), Letter of Administrative Restriction for IIM Accounts (the administrative restriction used to safeguard an IIM account until a Social Services Assessment has been completed) and a Notification of Administrative Restriction – IIM Account for Non-Responsiveness Code 19NR (non-responsive administrative restriction used when a Social Service provider has documented three unsuccessful attempted contacts with the guardian, conservator, representative payee, or client). Information shared may include the Account Holder's Name, Address, and decision regarding the account restriction.

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

Information may be shared with the Federal Bureau of Investigation (FBI) as part of an investigation for child protection or adult protection per Public Law 101-630.

Information may be cross-shared with the Social Security Administration (SSA) and the Veterans Affairs (VA) primarily in case management activities to determine eligibility for services.

Information may be shared with representatives of the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906, as authorized pursuant to the routine uses contained in SORN BIA-08, Financial Assistance and Social Services – Case Management System of records notice.

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

Some of the common programs the BIA social services staff work with to cross-share information includes,

- The state or Tribal Temporary Assistance for Needy Families (TANF) program;
- The State/County General Assistance Program;
- The local Food Stamps program, the Low Income Home Energy Assistance Program (LIHEAP), Tribal Housing Authority, Tribal/ State Day Care & Child Care Providers;
- Tribal/ State Child Welfare Agencies, Tribal/ State Foster Care Licensing Programs, State/ Tribal Schools, Local Law Enforcement Agencies both Tribal and State, depending on jurisdiction, Tribal/State Adult Protection Services, Tribal/ State behavioral health programs, medical providers, which may include Indian Health Services (IHS), Tribal/ State Courts.

Cross-sharing information is used primarily in case management activities to determine eligibility for services, as part of the investigation for child protection or adult protection and to facilitate services for the client, child, or family in alignment with the ISP and case plan, IIM Distribution Plan or court ordered treatment and services. This includes participating on child protection teams and multi-disciplinary teams with other tribal, state and federal programs.

There are also cross-reporting requirements outlined in Public Law 101-630 for Law Enforcement and Social Services programs to share information on Child Protective Services investigations. All documentation and information received from these organizations are documented in FASS-CMS Cloud as part of the client's case file, either through a document upload or a case note. Cross-sharing is on a "need-to-know" basis and is limited to information needed to coordinate services for clients.

☒ 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.

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

Information may be shared with third party vendors for foster care, kinship care, residential placement, group home placement, guardianship, and adoption subsidy; funeral services and other social services to enter into a contract for services and to make payments for services provided.

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 do have the option of not providing information when completing the Application for Financial Assistance and Social Services Form 5-6601. The information collected is used in determining an applicant's eligibility for financial assistance and social services provided by the BIA. Providing the information is voluntary. Not providing the information will result in the BIA not being able to determine eligibility to receive Federal program services and the Application for Services may be returned to the applicant to provide required information to make an appropriate assessment.

Individuals do have the option of not providing information when completing the Individual Self-Sufficiency Plan (ISP)/Case Plan Form 5-6602. The information collected is used to complete an individual self-sufficiency plan, which spells out the details necessary for a person to assume a meaningful job and must indicate the services received will meet the individual's and Tribal goals. Providing the information is voluntary. Not providing the information would result in the BIA not being able to complete the self-sufficiency plan and assist the individual in obtaining a meaningful job; and the individual may not be eligible for 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.

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

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

A Privacy Act Statement is provided to individuals when completing the Application for Financial Assistance and Social Services and the Individual Self-Sufficiency Plan/Case Plan.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through publication of this privacy impact assessment and the published system of records notice BIA-08, Financial Assistance and Social Services – Case Management System, 76 FR 56787; published September 14, 2011, 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.*

☒ 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.).

Records in FASS-CMS Cloud are primarily retrieved by Name and Case number. Records may also be retrieved by any other keyword search such as Date of Application, Mailing Address, Physical Address, Social Security Number, Taxpayer Identification Number (TIN), Date of Birth, Case Number, Financial and Business Management System (FBMS) Code, Tribal Affiliation, Tribal Enrollment number, Business Unit, Caseworker, and Vendor Name.

I. Will reports be produced on individuals?

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

25 U.S.C. 13, *the Snyder Act of 1924* (Pub. L. 101-630) requires Social Service staff to report cases of child abuse and neglect and refer to law enforcement agencies. This report may contain PII related to the child and family being investigated for child abuse and neglect purposes. PII included in this report may consist of Name of Child, Name of Child's Parents/ Caregiver, Name of Alleged Perpetrator, Type of Allegation, Child's DOB, Parent/Caregiver's DOB, Phone Number, Address, and Employment Information, Alleged Perpetrator's DOB, Phone Number, Address, and Employment Information, Date of Report of Allegation of Abuse & Neglect, Name of Reporter (the individual reporting the alleged child abuse and/or neglect), Reporter Narrative, CPS History for the child and alleged perpetrator, Name of Collateral Contacts, List of other Children in the home, child(ren)'s residency, and school information.

Caseworkers may prepare and use the Case Narrative Report that could potentially contain PII, which may consist of PII related to the child, parent/caregiver, and/or alleged perpetrator. PII included in these reports consists of the same information identified in the paragraph above. This report summarizes all the activity related to a specific client/case. This report is used by BIA staff for case assignment; or by Child Protection and Multidisciplinary Teams. A number of statistical reports are produced on child abuse and neglect which don't contain PII. Most reports generated in FASS-CMS Cloud are statistical reports and do not contain PII. Case workers are not able to modify or delete a case narrative, once it is entered in FASS-CMS Cloud.

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?

It is the responsibility of the client requesting services to provide accurate information. The client must also sign a fraud statement acknowledging responsibility for providing accurate information. Applicants or recipients who knowingly and willfully provide false or fraudulent information are subject to prosecution under 18 U.S.C. § 1001, which carries a fine of not more than $10,000 or imprisonment for not more than 5 years, or both. Additionally, per 25 CFR § 20.607, the social services worker is required to prepare a written report detailing information considered to be false and submit a report to the Superintendent or his/her designated representative for appropriate investigative action.

Case workers are also responsible for verifying the accuracy of the information submitted by the client. This may be done by contacting other Tribal, county, state, or federal agencies for verification along with crosschecking information against supporting documents provided by the client as proof of eligibility which may include SSN, Tribal Enrollment Card, passport and/or a

copy of their driver's license to show proof of identity; provides a copy of the their rental agreement; utility bill; or other housing bill to show proof of residency; provides a copy of their Individual Indian Money (IIM) account balance, bank account balance, and Social Security Administration benefit statement to show proof of income; and must provide a denial letter from other federal, state, tribal, or local programs to show the individual is not eligible for other programs.

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?

It is the responsibility of the client requesting services to ensure all information provided is complete and for submitting all required supporting documentation to the case worker. It is also the case worker's responsibility to validate all information and supporting documentation is complete before approving a client for services. FASS-CMS Cloud also assists with checking completeness through internal system data field checking which helps caseworkers verify required information and documentation is entered into FASS-CMS Cloud before payment is made to the client.

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).

It is the responsibility of the client requesting services to provide current information. Further, it is also the responsibility of the client to report any changes in the client's eligibility status. This is outlined in the client's Application for Financial Assistance and Social Services that they must sign when applying for services. Client information is updated on an ongoing basis between the clients and caseworkers.

25 CFR Part 20 states the BIA caseworker is responsible for conducting redetermination evaluations with the client every 3 months or 6 months. This process includes conducting home visits with the General Assistance (GA) clients or monthly site-visits to children in foster or residential care. This visit is an opportunity for the case worker to update client information. Additionally any time there is a change in the client's contact information an update process is initiated in FASS-CMS. Further, it is also the responsibility of the client to report any changes in the client's eligibility status including income, residency, etc. This is also outlined in the client's Application for Assistance that they must sign when applying for services. Client information is updated on an on-going basis between the case workers and clients. FASS-CMS Cloud updates the associated information in FBMS. This process ensures FASS-CMS Cloud information is synced with FBMS. This is accomplished thru an interface between FASS-CMS Cloud and FBMS that handles all payment related transactions.

User account information is provided directly by the user during account creation. 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.

Paper records are covered by Indian Affairs Records Schedule (IARS) Records Series 3600-Social Services and have been scheduled as permanent records under the National Archives and Records Administration (NARA) Job No. N1-075-05-001, approved March 31, 2005. Records are maintained under multiple file codes and may include program correspondence; general and child assistance case files, Indian adoption record files, social services reports, social service non-cash assistance information; Indian child Welfare Act (ICWA) review and grant files; Indian child welfare inquiry files, child protective service files, child welfare administrative review files, regional disbursement office reports, child abuse and neglect reports, social service invoice payment files; alcohol and substance abuse files and reports. Records are maintained in the office of records for a maximum of 5 years. Records are cut-off at the end of the fiscal year. The records are then retired to the American Indian Records Repository which is a Federal Records Center. Subsequent legal transfer of records to the National Archives of the United States will be as jointly agreed to between the United States Department of the Interior and the National Archives and Records Administration.

A records retention schedule for the electronic records in this system was developed by the Office of Trust Records (OTR) and has been submitted to NARA for review and approval, under 2200-Social Services Automated System (SSAS), NARA Job No. N1-075-07-015, July 30, 2007. Until the new schedule for FASS-CMS Cloud is approved, the 2200-SSAS schedule will be used to manage the FASS-CMS Cloud electronic records and master data, which are scheduled as Permanent.

FASS-CMS Cloud 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 FASS-CMS Cloud 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 Office of the Special Trustee for American Indians, Office of Trust Records, which provides support to include records management policies and procedures, and development of BIA's records retention schedule, records management policies and procedures. 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 FASS-CMS Cloud. FASS-CMS Cloud has undergone a formal Assessment and Authorization in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. FASS-CMS Cloud is rated as a FISMA moderate system and requires management, operational, and technical controls established by NIST SP 800-53 to mitigate the privacy risks for unauthorized access or disclosure, or misuse of PII that may lead to identity theft, fraud, misuse of credit, and exposure of sensitive information. FASS-CMS Cloud has a current System Security and Privacy Plan documenting required security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII maintained in the system.

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 is based on the "least privilege" principle combined with a "need-to-know" in order to complete assigned duties. BIA manages FASS-CMS 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 FASS-CMS 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 an understanding of the 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, protecting against inappropriate use or disclosure to unauthorized individuals.

There is a risk information that FASS-CMS Cloud 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. FASS-CMS Cloud meets BIA's information system security requirements, including operational and risk management policies.

There is risk of maintaining inaccurate information. This risk is mitigated by the following: (1) it is the responsibility of the client requesting services to provide accurate information. The client must also sign a fraud statement acknowledging responsibility for providing accurate information. Applicants or recipients who knowingly and willfully provide false or fraudulent information are subject to prosecution under 18 U.S.C. § 1001, which carries a fine of not more than $10,000 or imprisonment for not more than 5 years, or both. (2) Additionally, per 25 CFR § 20.607, the social services worker is required to prepare a written report detailing information considered to be false and submit a report to the Superintendent or his/her designated representative for appropriate investigative action; and (3) Case workers are also responsible for verifying the accuracy of the information submitted by the client. This may be done by contacting other Tribal, county, state, or federal agencies for verification along with crosschecking information against supporting documents provided by the client as proof of eligibility which may include SSN, Tribal Enrollment Card, passport and/or a copy of their driver's license to show proof of identity; provides a copy of the their rental agreement; utility bill; or other housing bill to show proof of residency; provides a copy of their Individual Indian Money (IIM) account balance and bank account balance to show proof of income; and must provide a denial letter from other federal, state, tribal, or local programs to show the individual is not eligible for other programs.

There may be a risk associated with the collection of information from other DOI systems. This risk is mitigated as FASS-CMS Cloud and FBMS interface via an encrypted, secure file transfer protocol. FASS-CMS Cloud creates new/updates contact and vendor records and the approval/authorization of payments, generates transmission of the record to FBMS. FBMS then responds with a file which contains FBMS new vendor identifiers, confirmation information to update vendor information, and the rejection of payment information to FASS-CMS Cloud.

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 regards to information handling and retention procedures, the Division of Human Services is responsible for managing and disposing of BIA records in FASS-CMS Cloud 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. The Division of Human Services ensures only those records needed to support its program, Tribes, and Tribal members is maintained. The Division of Human Services maintains the records for a maximum of 5 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 Codes N1-075-05-001 (3600-Social Services) and N1-075-07-015 (Series 2200 – SSAS). Information collected and stored within FASS-CMS Cloud 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 notice of the purposes for collecting their information. This risk is mitigated as individuals are notified of the privacy practices through this PIA and through the published SORN BIA-08, Financial Assistance and Social Services – Case Management System, 76 FR 56787; published September 14, 2011, which may be viewed at which may be viewed at https://www.doi.gov/privacy/bia_notices. Additionally, Privacy Act Statements (PAS) are part of the Application for Financial Assistance and Social Services and the Individual Self-Sufficiency Plan (ISP)/Case Plan. 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 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. FASS-CMS Cloud is hosted and administered within a DOI-approved and FedRAMP-certified hosting center. The cloud service provider has implemented 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 Bureau maintains an audit trail of activity sufficient 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 gain an understanding of the responsibility to protect an individual's 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 use of the system and data collected is relevant and necessary to the purpose for which FASS-CMS Cloud was designed to align with and support the requirements identified in 25 CFR Part 20, Financial Assistance and Social Services programs.

☐ 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. FASS-CMS Cloud 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*

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 FASS-CMS Cloud 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 FASS-CMS Cloud user accounts. Federal employee access requires supervisor, system/business owner, and system administrator approval. Contract officer representatives determine the level of access for contractors, which is approved by the information owner. Tribes who have contracted or compacted a government trust function may submit requests for access for tribal members working on a program, which must be approved by the program manager.

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 clause was included in the contract: FAR 52.239-1, Privacy or Security Safeguards (Aug 1996). However, all required contract clauses will be included in the next contract update.

☐ 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 FASS-CMS Cloud 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.

☐ No

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

The FASS-CMS Cloud 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?

FASS-CMS Cloud 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. FASS-CMS Cloud 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. FASS-CMS Cloud assigns roles based on the principle of "least privilege" and performs due diligence toward ensuring that separation of duties is in place.

In addition, all users are required to consent to FASS-CMS Cloud 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 and annually, to ensure they have an understanding of their responsibility to protect privacy.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. In accordance with applicable DOI guidance, FASS-CMS Cloud maintains an audit trail of activity sufficient to reconstruct security relevant events. The audit trail includes system user 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 (ACIO) is the Information System Owner (ISO). The 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 FASS-CMS Cloud. 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 FASS-CMS Cloud ISO and ISSO are responsible for oversight and management of the FASS-CMS Cloud 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 FASS-CMS Cloud 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 one 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. In accordance with the Federal Records Act, the Office of Trust Records is responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.