U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

MINC

OCFO-ACFO-SS

DAITO

Date PIA submitted for review:

June 4th 2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Michele Washington	michele.washington@usda.gov	202-205-3369
Information System Security Manager	Kenneth McDuffie	kenneth.mcduffie@usda.gov	504-982-6234
System/Program Managers	Linda Connolly	Linda.connelly@usda.gov	202-674-9137

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Assistance Chief Financial Officer – Financial Management Systems (ACFO-SS-FMS) Miscellaneous Income (MINC) system. The PIA was conducted because the MINC system has the potential to store personally identifiable information within the cloud provided solution.

Overview

System Name: MINC

USDA Component: Office of the Chief Financial Officer

The miscellaneous income (MINC) application manages 1099 information and produces 1099 forms to provide to taxpayers and files to provide to the IRS for tax reporting purposes. The MINC application aggregates 1099 data from four sources (i.e., FMMI, EARN, SPPS, & US Bank) throughout the calendar year and generates reportable 1099 forms (i.e., Amounts over $600) that are sent to the taxpayer and a corresponding file containing that information that is sent to the IRS. Corrections are also recorded and reported throughout the year, with a correction file sent to IRS at mid-year (i.e., August).

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

- Chief Financial Officers Act of 1990 (Pub. L. 101–576
- 26 U.S.C. Section 6011, General requirement of return, statement, or list.
- 26 U.S.C Section 6109, Identifying Numbers.
- 31 U.S.C. 3711 through 3719, Claims of the United States Government.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

The system was formerly Accredited through the Risk Management Framework process of the USDA. CSAM contains all the proper documentation. The Authority to Operate date is February 17, 2023, with an expiration date of February 17, 2026.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

USDA/OCFO-10, Financial Systems, published at 83 FR 67712 (January 1, 2019).

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No, the information collected does not apply to government workers or contractors when they are collecting information as part of their official duties. This is because government workers and contractors are considered to be agents of the government, and the government is exempt from the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

MINC is a web-based financial management software application used by USDA to calculate, process, manage and report on all the Department's financial transactions (i.e., payments) associated with the reporting of 1099 data to taxpayers and the Internal Revenue Service (IRS). These transactions include the reporting of payments for interest, grants and miscellaneous income. The application provides assurance of compliance with agency and federal regulations, automated and accurate calculations, and comprehensive reporting.

Payments by the USDA for grants, interest, and miscellaneous income are input into the MINC system on a monthly, quarterly, and annual basis. The application accumulates payment data by vendor and payment type. At the end of the tax year, the application produces 1099 forms based on business rules for sending to taxpayers. The application also produces an electronic file of the same information that is sent to the IRS. Throughout the subsequent year, MINC users apply corrections provided by taxpayers to 1099 data. At mid-year, the corrections file is sent to the IRS.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers			
☒	Social Security number	☐	Truncated or Partial Social Security number
☐	Driver's License Number	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☒	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☒	Employee Identification Number	☐	Professional License Number
☒	Taxpayer Identification Number	☒	Business Taxpayer Identification Number (sole proprietor)
☒	Credit/Debit Card Number	☒	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number	☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)

☐	Personal Device Identifiers or Serial Numbers			☐	Business device identifiers or serial numbers (sole proprietor)
☐	Personal Mobile Number			☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number				
Biographical Information					
☒	Name (including nicknames)	☐	Sex	☐	Business Mailing Address (sole proprietor)
☒	Date of Birth (MM/DD/YY)	☐	Ethnicity	☐	Business Phone or Fax Number (sole proprietor)
☒	Country of Birth	☒	City or County of Birth	☐	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☐	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☐	Spouse Information	☐		☐	Children Information
☐	MaMINCl Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☒	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)
☐	Employment Information	☐	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight
Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information

☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

2.2. What are the sources of information in the system/program?

The contractor and/or vendor information within the system is obtained from feeder systems i.e., EARN, FMMI, SPPS and US Bank.

2.2.1. How is the information collected?

MINC aggregates 1099 data from four sources (i.e., EARN, FMMI, SPPS and US Bank) throughout the calendar year and generates reportable 1099 forms (i.e., amounts over $600) that are sent to the taxpayer and a corresponding file containing that information that is sent to the IRS. Corrections are also recorded and reported throughout the year, with a correction file sent to IRS at mid-year (i.e., August). MINC manages 1099 information and produces 1099 forms to provide to taxpayers and files to provide to the IRS for tax reporting purposes.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

Yes. MINC aggregates 1099 data from four sources (i.e., EARN, FMMI, SPPS and US Bank) throughout the calendar year and generates reportable 1099 forms (i.e., amounts over $600) that are sent to the taxpayer and a corresponding file containing that information that is sent to the IRS.

2.4. How will the information be checked for accuracy? How often will it be checked?

Not applicable. MINC receives 1099 data from feeder systems (i.e., EARN, FMMI and SPPS) and does not directly collect information from individuals.

2.5. Does the system/program use third-party websites?

Not applicable

2.5.1. What is the purpose of the use of third-party websites?

Not applicable

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

Not applicable

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of Information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Non-compliance with Regulations: Failing to accurately characterize information can lead to non-compliance with privacy laws and regulations, resulting in legal penalties and reputational damage.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

ACFO-FMS does not collect information from individuals. MINC receives 1099 data from feeder systems (i.e., EARN, FMMI, SPPS and US Bank). The information

received and maintained will include contractor or vendor's full name, address; social security number; tax identification number; and financial data (credit card numbers, bank account numbers, etc.).

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Overuse of Information: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Loss of Data Control: When PII is shared with third parties, there is a risk of losing control over how that data is used, potentially leading to unauthorized access or exploitation.

Increased Risk of Data Breaches: The more PII is used and shared, the higher the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Mitigation: By implementing some or all the following mitigation actions, mission areas may safeguard PII better and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.
User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Transparency: Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.

Regular Training: Provide regular training for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

This system provides notice via SORN. USDA/OCFO-10, Financial Systems, published at 83 FR 67712 (January 1, 2019).

4.2. What options are available for individuals to consent, decline, or opt out of the project?

Users are not able to consent, decline, or opt out of usage of the system due to their consent to provide the information through the listed feeder systems.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Mitigation: MINC provides notice through the listed SORN. the SORN and is a publicly available document. USDA/OCFO-10, Financial Systems, published at 83 FR 67712 (January 1, 2019).

Also, implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5.0 Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

Information is retained in compliance with NARA retention guidelines for financial management data. Bill related data is retained for a minimum of six full years.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

The retention period has been approved by the component records officer and the National Archives and Records Administration (NARA). The name of the records retention schedule is General Records Schedule 1.1 (GRS 1.1).

The relevant data is covered in the following sections of GRS 1.1:

- Financial Management and Reporting Records: This section covers records related to procuring goods and services, paying bills, collecting debts, and accounting for financial transactions.

- Financial Transaction Records: This section covers records related to procuring goods and services, paying bills, collecting debts, and accounting for all financial activity.

- Accounting Records: This section covers records related to the recording, classifying, and summarizing of financial transactions and events.

GRS 1.1 provides specific retention periods for different types of financial records, based on factors such as the type of record, its purpose, and its legal and regulatory requirements.

5.3. PRIVACY IMPACT ANALYSIS: **Related to retention of information.**

Follow the format below:

Privacy Risk: Privacy act risks associated with the retention of information include:
Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Non-compliance with Regulations: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

Increased Legal Risks: Long retention periods can increase the risk of being involved in litigation, as older data may be subjected to subpoenas or discovery requests.

Mitigation: Implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Access Controls: Implement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

MINC receives 1099 data from feeder systems (i.e., EARN, FMMI and SPPS) and is used by the OCFO/ ACFO-SS/FMS Process Services Branch (PSB) of the United States Department of Agriculture. The PSB uses the information to correct 1099's and answer customer inquiries. MINC receives 1099 data from feeder systems (i.e., EARN, FMMI and SPPS) through a secure interface. The final 1099's are mailed to individuals.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: MINC receives 1099 data from feeder systems (i.e., EARN, FMMI and SPPS).

Mitigation: Users are USDA employees who have undergone background checks and receive annual Security Awareness training and privacy training.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Financial and PII data is shared with the following organizations, for the purpose of

accurate accounting transactions:

- Department of the Treasury, for monetary disbursements.
- Internal Revenue Service, for tax reporting and collection.
- Office of Management and Budget, for USDA financial reporting.
- Contractor responsible for printing the 1099's forms for mailing.

Information is shared almost exclusively via secured electronic file transfer. All interconnections are safeguarded through security measures defined within the established Memorandum of Understanding and/or Interconnection Security Agreements. Security controls applied to system interconnections are assessed annually to verify and validate that security protections are operating as intended.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.
Follow the format below:

Privacy Risk: Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Non-compliance with Regulations: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.

Inconsistent Data Management Practices: Different third parties may have varying practices for handling PII, leading to inconsistencies in data protection and increased risks.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Data Sharing Policy: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Need-to-Know Basis: Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

Individuals seeking notification of and access to any record contained in this system of records, may submit a request in writing to the Headquarters or Components FOIA Officer, whose contact information can be found at https://www.dm.usda.gov/foia/poc.htm. FOIA inquiries for the FOIA should be directed to:

FOIA Director
Email: USDAFOIA@usda.gov

7.2. What are the procedures for correcting inaccurate or erroneous information?

Individuals will need to contact the owners of the aforementioned systems to ensure the accuracy of the information collected about them. Any update(s) to the information within these systems will also be reflected within MINC when it receives updated 1099 data from the feeder systems.

7.3. How are individuals notified of the procedures for correcting their information?

The USDA/OCFO-10, Financial Systems, SORN provides methods for correcting their information. Freedom of Information Act (FOIA) Division inquiries for the Office of Information Affairs (OIA) should be directed to the OIA Director.

7.4. If no formal redress is provided, what alternatives are available to the individual?

Individuals seeking notification of and access to any record contained in this system of records, may submit a request in writing to the Headquarters or Components FOIA Officer, whose contact information can be found at https://www.dm.usda.gov/foia/poc.htm. If an individual believes more than one Component maintains Privacy Act records concerning him or her the individual may submit the request to Chief FOIA Officer, Department of Agriculture, 1400 Independence Avenue SW, Washington, DC 20250. When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 7 CFR part 1.112. You must verify your identity, meaning that you must provide your full legal name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is

required, you may obtain forms for this purpose from the Chief FOIA Officer, Department of Agriculture, 1400 Independence Avenue SW, Washington, DC 20250. In addition, you should provide the following:

- An explanation of why you believe the Department would have information on you
- Identify which Component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which USDA Component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, the Components(s) may not be able to conduct an effective search and your request may be denied, due to lack of specificity or lack of compliance with applicable regulations.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Delayed Responses: Slow responses to redress requests can frustrate individuals and exacerbate feelings of mistrust and dissatisfaction, potentially leading to reputational harm.

Inconsistent Application: If redress processes are applied inconsistently across different cases or agencies, it can lead to perceptions of unfairness and bias, undermining trust in the entire department.

Mitigation: Implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Timely Response Protocols: Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued.

Section 8 Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

8.1. How is the information in the system/project/program secured?

MINC is protected behind Virtustream firewall network defense system which continuously monitors suspicious activities. On behalf of ACFO-FMS, Virtustream tracks application transaction logging to provide, at a minimum, failed login attempts, unauthorized access, the capability to capture a copy of each transaction record to include changed data and reflecting the user identification (ID) of the individual initiating or changing a record. The log is protected from unauthorized modification, destruction, and access by the limiting access rights to audit logs.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?