USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed "Gender" and "Sexual Orientation" from Biographical Information in accordance with Executive Order 14168, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government."

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	(LSAS)
Program Office	FSIS
Mission Area	Food Safety
CSAM Number	1895
Date Submitted for Review	20 May 2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Keith Komosinski	keith.komosinski@usda.gov	863-220-4182
Information System Security Manager	Rodney Sallie	rodney.sallie@usda.gov	202-708-9528
System/Program Managers	Shayla Bailey	shayla.bailey@usda.gov	202-690-6188

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

This document serves as the Privacy Impact Assessment (PIA) for the United States Department of Agriculture (USDA) Label Submission and Approval System (LSAS). The purpose of the system is to support the submission, evaluation, and adjudication of labeling application packages. LSAS will provide the means to extract selected records from the entire LSAS database. This assessment is being done in conjunction with the LSAS Privacy Threshold Analysis and is reviewed annually.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

LSAS is a web-based software application that integrates and implements an electronic label application process for establishments to submit label applications and appeals. The LSAS application standardizes, formalizes and automates the paper-based business label submissions process for approval from the meat, poultry, and egg products establishments. The LSAS system integrates and streamlines the following actions: submit, transport, distribute, and evaluate. All label requests are handled by these four major processes. Through LSAS, LPDS will view, evaluate, and adjudicate all electronically submitted label application packages (LAPs) and appeal packages (APs). It keeps a record of pertinent review decisions information for each label that has been processed, and generates reports based on the label information stored in the system. The LSAS application serves as a searchable database when seeking information about products or establishments.

Users of LSAS are from within USDA and authorized industry users. USDA users are from FSIS (LPDS and Inspection Personnel) and Agriculture Marketing Services (AMS). Industry users include mostly establishments and, to a lesser extent, expediters.

The LSAS solution provides the importation/conversion of legacy data records from the Label Information System (LIS), including the semi-automated optical character recognition of legacy application multi-page TIFF format images, which includes text-within-graphic conversion and freehand character recognition. LSAS provides the means to extract selected records from the entire LSAS database, both directly through a query-type interface, and as a data source for external systems. LSAS empowers senior leaders with internal management controls to evaluate work performed by their subordinates and perform quality control reviews before finalizing the adjudication of labeling applications. LSAS allows auditing activities on established user accounts or events and generate audit records.

LSAS interfaces with standard FSIS information management tools and service-oriented architecture utilizing web services. LSAS leverages FSIS User Interface (UI) Framework and complies with FSIS Architecture Framework guidelines. LSAS utilizes USDA's e-

Authentication system for system access control and FSIS Authorization Web Service. LSAS functionalities leverage the "Common Service" available within the FSIS Enterprise Network, such as: Logging, Authorization, User and Event Notification, Error Handling, and Business Rule Engine Services.

Online electronic transactions are performed by authorized users of the LSAS application from workstations connected to the FSIS intranet. Role-based access to application functionality is provided via components of the FSIS .NET Framework infrastructure. Remote users connecting via the Internet authenticate themselves to the USDA eAuthentication system for secure connectivity to LSAS. USDA's eAuthentication system authenticates all user logins to the FSIS intranet and to their authorized applications. Site Minder works with eAuthentication to support user authentication to the application and to monitor session validity

The legal authority to operate for LSAS is provided by the signed Authority to Operate (ATO) letter dated 10/27/2026.

Section 1: 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?

The authorities for USDA to collect, maintain, use and disseminate information through this system are under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901- 1906).

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

Yes

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

LSAS receives PII from NFC, it operates under the departmental NFC System of Records Notice (SORN), OCFO_NFC-1.

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

N/A

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

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

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

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
☐ Passport number	☐ License Plate number	☐ Registration number
☒ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☒ Employee Identification number	☐ Alien Registration number	☐ DOD ID 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

☐ Health Plan Beneficiary number
☒ Business Mobile number (sole proprietor)
☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)
☒ 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
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☒ Home Phone or Fax Number

☒ Home Address
☒ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☐ Military Service Information

☐ Race
☐ Nationality
☐ Mother's Maiden Name

☒ Personal Email Address
☒ Business Email Address
☐ Global Positioning System (GPS)/Location Data

☒ Employment Information
☐ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☐ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☒ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

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

[Pay Plan, Grade, Step, EOB, Job Number, Title, Duty Station Code, Supervisory Code, Series, Series Description, Full Organizational Code, UID, New Employee UID, Last Updated]

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

The sources of this information are the forms provided by the establishment or a business entity acting on behalf of the establishment, legacy data previously provided by these entities to FSIS, and the comments made by FSIS reviewers of those forms.

2.2.1. How is the information collected?

The data is obtained from FSIS Form 7234-1, Application for Approval of Labels, Marking or Device and NFC feeds. An automated job that executes queries in NFC's reporting tool, Insight, is run daily. This job authenticates with an account created specifically for this purpose and retrieves all the data configured for use by LSAS and inserts or updates it in the application's databases.

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

No

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

Meat, poultry, and processed egg product establishments are responsible for accurately labelling their product for human consumption. The labels are reviewed and must be approved by the appropriate LPDS staff. LSAS will have built-in data verification checks and some pre-populated date fields. The date fields, along with the LPDS user identification (ID), will be part of the electronic history of each record.

2.5. Additionally, NFC and its systems manage all employee data and conduct accuracy checks to ensure the information is correct and reliable on their daily run.Does the system/program use third-party websites?

No

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

2.6. **Privacy Impact Analysis**: Related to characterization of the 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.

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: 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?

The information provided by the customer will help ensure labels for meat, poultry, and processed egg products are accurate, and not misleading. Accurate labeling helps to protect customers who have allergies or other food sensitivities. The information will also help to protect consumers from any misbranded and economically adulterated meat, poultry, and egg products. LPDS is responsible for checking and verifying the labels comply with federal statutes, regulations and directives.

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.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

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

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

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.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses 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?

Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for PII for all Source System users. Plant vendors are provided notification during business agreement processes. Additionally, users access the LSAS application via eAuthentication accounts. The eAuthentication login page includes a link to the USDA's privacy notice, and is available to every user when they log in.

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

N/A

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.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act 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: 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?

Data is maintained until they become inactive per NARA requirements, minimum 2 years, and at which time they will be destroyed, retained no longer than 5 years, or retired in accordance with the Department's published records disposition schedules, as approved by the NARA

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.

Yes. LSAS uses the DAA-0584-2019-0005 retention schedule

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.

Mitigation: To mitigate these risks, LSAS has adopted a data retention policy that emphasizes limited retention periods, secure storage practices, regular audits of stored data, timely deletion of unnecessary information, and transparency with users regarding their data handling practices. Additionally, LSAS has implemented strong security measures to safeguard-retain data from unauthorized access.

Section 6: 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?

LSAS shares connection with:

- Azure N-GSS: HR-GSS's Hosting System
- Enterprise Active Directory: User Authentication
- ICAM Shared Services: User Authorization
- Insight: Connection with National Finance Center (NFC)
    - The bulk of the PII within HR-GSS is provided by the network connection to Insight. This information is necessary for Human Resource Purposes.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Privacy risks associated with internal sharing and disclosure include:

Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

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.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

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?

No Information containing PII is shared with organizations external to the USDA.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: LSAS does not share data externally with entities or organizations. Information collected by LSAS is used exclusively for communication purposes.

Mitigation: Under normal operations, employee PII is not shared externally. It is only disclosed if legally required, following standard FSIS or USDA data protection guidelines.

Section 7: 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 who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests.

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

Individuals can contact their offices or an LSAS staff member to correct their PII. LSAS staff members who make PII corrections have a "need to know" and are authorized to correct PII errors. Also, the LSAS application has a messaging mechanism through which applicants can send requests to correct their PII. Other options include sending an email or calling an LSAS member.

Any individual who has reason to believe that LSAS might have inaccurate or erroneous PII records pertaining to him or her should be written to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 -Phone: (202) 720-2109 Fax (202) 690-3023 - Email: fsis.foia@fsis.usda.gov.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice on both Form 7234-1 and Form 8822-4. The individual's acknowledgement of the Privacy Act Notice and the proof of information signify the individual's consent to the use of the information. The purpose, use, and authority for collection of information are described in the Privacy Act Notice

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

N/A – Formal redress is provided

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.

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.

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?

LSAS enforces encryption, controls access based on eAuthentication, forces a timeout after a specified period of inactivity, and maintains system audit logs.

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

The majority of external LSAS users are the submitters followed by the internal USDA users from two program areas: FSIS LPDS and AMS. Access to LSAS is only granted to individuals from these program areas who are involved in the label submission and approval life cycle process. Access is strictly controlled and is based on business needs. LSAS is a role-based system. When users access LSAS, the functionality and data to which they have access is dependent on their role and assignments in LSAS. There are various classes of users who will interact with LSAS. Factors that define a user class include responsibilities, skill level, work activities, and mode of interaction with the system. User roles assigned within LSAS determine the permissions granted. The options available on the left side, Navigation Panel, of LSAS' Home page and the functions that can be accessed vary based on the LSAS role. LSAS provides "Submitter" role for Industry users. LSAS utilizes a one-time enrollment process for external users (Industry, establishments, expeditors, label consultants, and small businesses, etc.). User authentication is the foundation of LSAS' role-based access. Each user's screen display, privileges and the scope of functionality is based on their specific work assignments, responsibilities, and role within LSAS. The procedures governing the roles and access to LSAS are documented in the FISMA Assessment and Authorization (A&A) documents for LSAS, such as System Security Plan and Access Control SOPs.

8.3. How does the program review and approve information sharing requirements?

This is Not Applicable because LSAS does NOT share information

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

Regular, recurring security training which has a privacy component is conducted. All internal users, including contractors, are required to undergo Department-approved Computer Security Awareness and Training prior to being granted access and annually thereafter to retain access.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 7/22/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed: TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.07.23 06:05:02 -04'00'

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:_____

Rosalyn LeeAnn Murphy
System Owner
FSIS
U.S. Department of Agriculture

Signed:_____

Keith Komosinski
Mission Area Privacy Officer
FSIS
U.S. Department of Agriculture

Signed:_____

Marvin Lykes
CISO/ACISO
FSIS
U.S. Department of Agriculture