Privacy Impact Assessment

USDA Label Submission and Approval System (LSAS)

- Version: 12
- Date: October 1, 2020
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Label Submission and Approval System (LSAS)

October 1, 2020

Contact Point

Rosalyn Murphy-Jenkins
Director
Labeling and Program Delivery Staff (LPDS)
Office of Policy and Program Development
USDA Food Safety and Inspection Service (FSIS)
Patriots Plaza III
355 E. Street SW 9-148
Washington, DC 20024
301-504-0878

Reviewing Official

Timothy Poe

FSIS Privacy Office

(202) 260-9433

United States Department of Agriculture

Revision History

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
5.0	03/25/2014	Marie Penninger	Annual Review/Updated signatures not required until ATO
6.0	09/10/2014	Marie Penninger	ATO update
7.0	03/11/2016	Rohan A. Heath	Annual Review/Update – No signatures required until ATO
8.0	03/07/2017	Tope Ayodeji	Annual Review/Update – No signatures required until ATO
8.1	10/18/2017	Tope Ayodeji	FY18 ATO Update
8.2	01/17/2018	Tope Ayodeji	SO Review for FY18 ATO
8.3	01/18/2018	Tope Ayodeji	Privacy Office Review for FY18 ATO
8.4	01/23/2018	Tope Ayodeji	CISO Review for FY18 ATO
9.0	03/23/2018	Erik Nudo	CIO Review and Signature for FY18 ATO
9.1	11/14/2018	Kathryn Stuart	FY19 Annual Review and Update (Consolidated and Finalized updates from System Stakeholders)
10.0	04/08/2019	Kathryn Stuart	FY19 Assessment Complete – Finalized Docs
10.1	08/05/2019	Kathryn Stuart	FY20 Update and Review for Annual Assessment
10.2	02/13/2020	Kathryn Stuart	Incorporated FY20 system stakeholder updates
11	07/01/2020	Kathryn Stuart	Finalized document at conclusion of FY20 A&A cycle

12	10/01/2020	Trang Nguyen	Reviewed and Updated for FY21 A&A

Abstract

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

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 review before finalizing the adjudication of labeling applications. LSAS allows auditing activities on established user accounts or events and generate audit records.

LSAS interfaces with the 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 03/27/2018.

Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

The information being collected consists of establishment name, e-mail, business address, and signature of the applicant. If the establishment is represented by an agent (expeditor) then name, e-mail address, business address, telephone number, and the signature of the agent is collected. The information collected comes from FSIS Form 7234.1 entitled *"Application for Approval of Labels, Marking or Device."* This form also includes information pertaining to product identification, claims, net weight, species identification, and nutrition related to meat, poultry and egg products, formulations, processing procedures, ingredients, and special claims and from FSIS Form 8822-4 *"Request for Label Reconsideration."*

1.2 What are the sources of the information in the system?

Source 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.

1.3 Why is the information being collected, used, disseminated, or maintained?

Under the Code of Federal Regulations (CFR) 9 CFR 320.1(b) (11) and 381.175(b) (6), records of all labeling, along with the product formulation and processing procedures, are maintained. The information provided by the customer will help ensure labels for meat, poultry, and processed egg products are safe for human consumption, accurate, and not misleading. The information will also help to protect consumers from any misbranded and economically adulterated meat, poultry, and processed egg products.

1.4 How is the information collected?

The data is obtained from FSIS Form 7234-1*, Application for Approval of Labels, Marking or Device.*

1.5 How will the information be checked for accuracy?

Meat, poultry, and processed egg product establishments are responsible for accurately labeling 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.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14,

In addition, USDA is generally authorized to collect information to support its mission 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).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

LSAS users access the system using unique, authorized USDA eAuthentication Level 2 accounts. LSAS cannot be accessed without an authorized account. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user; this ensures least privileges are enforced.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and Office of Management and Budget (OMB) Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every 3 years. USDA Enterprise Active Directory vice FSIS Active Directory and LSAS role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When internal users (FSIS employees and contractors) are granted access to the FSIS environment, they are issued a USDA e-mail account and an FSIS user account (managed in Active Directory). When a user accesses LSAS, there are specific user roles that are used to further restrict a user's access. FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer (OCIO), FSIS.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., software developers) are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are experts in such matters.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

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.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Label data is available inside LSAS to allow LPDS to run reports for individual submission, summarized data analysis, and management controls. Crystal reports, which is a commercial reporting software tool, is used to design and generate reports used for data analysis. LSAS has the capability to run internal reports, such as canned reports (trend reports, management controls for audit purposes), as well as ad-hoc reports in response to recalls, specific ingredients of concern, and congressional.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

LSAS does not use commercial (purchased or subscribed data feed from third party sources) or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

LSAS utilizes firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for IT. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act, subsection e [9], and OMB Circular A-130, Appendix III. All of the security controls in the system are reviewed when significant modifications are made or at least every three years. The SSP, and a subset of these controls, is also reviewed annually.

In addition, privacy risks are minimized as information collected is predominantly business related. Access to data is strictly controlled. Access is granted through the USDA approved secure single sign on application (eAuth – Level 2 access) and authorization within LSAS is role based to ensure least privileges.

Authorized user login identifiers are appended to system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture, FSIS systems, and security.

Section 3.0 Retention

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

3.1 How long is information retained?

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.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The length of time data is retained does not change the level or type of risk associated with data retention. LSAS enforces encrypted, controlled access based on eAuthentication, timeout for remote access, and system audit logs to ensure information is handled in accordance with the above described uses. All authorized staff using the system must comply with the Agency's general use policy for IT. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act, subsection e [9], and OMB Circular A-130, Appendix III.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Label information is shared with FSIS inspection personnel (limited by their establishment assignment) and authorized users from Agriculture Marketing Services (AMS) who are responsible only for administering the Child Nutrition Program (CNP) labels within LSAS. AMS users have access to CNP labels only.

4.2 How is the information transmitted or disclosed?

FSIS inspection personnel and AMS personnel have direct access to LSAS after logging in via eAuthentication.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Access to data is strictly controlled. Access is granted through the USDA approved secure single sign on application (eAuth – Level 2 Access) and authorization within LSAS is role based to ensure least privileges.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information is not shared with organizations external to the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

LSAS does not share PII outside of the Department.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

N/A.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

N/A.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL?

No.

6.2 Was notice provided to the individual prior to collection of information?

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (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.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes, but label approval may be predicated on provision of the information. LSAS treats, and safeguards, all information with the same rigor.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to consent to particular uses of the information.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The OMB statement is prominently displayed at the beginning of the information collection process.

Section 7.0 Access, Redress and Correction

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

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 write 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 the Form 7234-1 and Form 8822-4. The individual's acknowledgement of the Privacy Act Notice and the proffer 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: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Corrections to the data are securely maintained in the same manner as the original data; therefore, there is no privacy risk associated with redress available to individuals.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system 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.

8.2 Will Department contractors have access to the system?

Yes, authorized departmental contractors will have access to the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are experts in such matters.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

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.

8.4 Has Assessment & Authorization been completed for the system or systems supporting the program?

LSAS went through the A&A process and an ATO was granted on 03/27/2018 and will expire on 03/27/2021.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

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

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks are minimized as primarily, onlybusiness names and addresses, with limited individual names, are collected. All authorized staff using the system must comply with the Agency's general use policy for IT known as "Rules of Behavior and Consequences." System use notifications are in accordance with the Privacy Act, subsection e[9], and OMB Circular A-130, Appendix III.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

LSAS is a web-based application for FSIS.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

No, the project does not employ technology which may raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

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

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

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

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

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

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

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

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

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

If so, is it done automatically?

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

If so, is it done on a recurring basis?

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

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

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

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

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

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

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

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

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

Responsible Officials

Rosalyn Murphy-Jenkins,
System Owner (SO) - LSAS
Director - Labeling and Program Delivery Staff (LPDS)
Office of Policy and Program Development, USDA, FSIS,
Patriots Plaza III
355 E. Street SW, 9-148
Washington, DC 20024

Marvin Lykes
Chief Information Security Officer
1400 Independence Ave., SW
Washington, DC 20250

Timothy Poe
Privacy Office
1400 Independence Ave., SW
Washington, DC 20250

Carl A. Mayes
FSIS Assistant Chief Information Officer
1400 Independence Ave., SW
Washington, DC 20250

Approval Signatures

ROSALYN MURPHY JENKINS

Digitally signed by ROSALYN MURPHY JENKINS
Date: 2021.03.01 09:36:55 -05'00'

Rosalyn Murphy-Jenkins
System Owner

DATE

MARVIN LYKES

Digitally signed by MARVIN LYKES
Date: 2021.03.02 10:37:02 -05'00'

Marvin Lykes
Chief Information Security Officer

DATE

TIMOTHY POE (Affiliate)

Digitally signed by TIMOTHY POE (Affiliate)
Date: 2021.03.01 12:20:27 -05'00'

Timothy Poe
Privacy Office

DATE

CARL MAYES

Digitally signed by CARL MAYES
Date: 2021.03.04 14:39:53 -05'00'

Carl A. Mayes
FSIS Assistant Chief Information Officer

DATE