

Privacy Impact Assessment

Label Information System

- Version: V2.5
- Date: September 12, 2012
- Prepared for: USDA OCIO FSIS





Document Revision and History			
Revision	Date	Author	Comments
2.0	February 2007	Diane St.Clair	Reformatted & re-organized
2.1	March 2, 2007	Marc Brown	Edited to reflect elimination of electronic processing of label images
2.2	March 2, 2007	Kevin O'Donovan	Final proofread
2.3	March 27, 2007	Marc Brown	Interchange phone numbers of Lynn Yoder and Robert Post
2.4	June 4, 2012	Ameya Thatte	Annual update
2.5	September 12, 2012	Kenneth Hopson	Addressed and updated with PO comments

Abstract

This document serves as the Privacy Impact Assessment for the USDA Label Information System (LIS). The purpose of the system is sampling and compliance verification, tracking and analyzing generic approval audits for label accuracy, and documenting approval decisions. This auditing of labels helps to ensure that FSIS may continue to accomplish its mission of ensuring a safe and wholesome food supply for the Nation's population. This assessment is being done in conjunction with the LIS Privacy Threshold Analysis.

Overview

The LIS is owned by the Food Safety and Inspection Service, Office of Policy and Program Development, Labeling Program and Delivery Division (LPDD).

The LIS tracks meat, poultry, and egg product label applications submitted by domestic and foreign Federal meat and poultry establishments. The system is used for sampling and compliance verification, tracking and analyzing generic approval audits for label accuracy, and for documenting approval decisions. This auditing of labels helps to ensure that FSIS may continue to accomplish its mission of ensuring a safe and wholesome food supply for the nation's population

LIS is a multi-user, interactive, on-line computer system that tracks the status of a label application under the control of the LPDD, keeps a record of pertinent review decision information for each label that has been processed through the system, and generates reports based on the label information stored in the system.

LIS records include the following:

- Labels by Current Date
- Totals by Status
- Totals by Submission Code
- Label Information Queries by Expeditor
- Pending Label Application Report
- Total Labels Processed (Domestic/Foreign)
- Labels on Hold by Reviewer
- Label Information Queries by Plant
- Label Decisions Appeal
- Appeal Totals
- Employee Counts

- Foreign Establishment Database
- Label applications
- Labels
- Formulations
- Processing Procedures
- Ingredients

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?

LIS collects the following PII information:

- Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, user ids etc.)
- Handwriting or an image of the signature
- Name and work location contact information of applicant

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

The LPPD receives paper-based application forms from through U.S. mail, fax, in person, or by courier from the various businesses requiring approval of their labels.

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 that labels for meat, poultry, and processed egg products are safe for human consumption, accurate, and not misleading. The information also helps to protect consumers from any misbranded or 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. Label applications come in to the LPDD staff through U.S. mail, fax, in person, or by courier from the various businesses requiring approval of their labels. LPDD receives approximately 300 labels daily.

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 LPDD staff. LIS will have built-in data verification checks and some pre-populated date fields. The date fields, along with the LPDD user 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?

Federal regulations for meat, poultry, and egg product labels are covered in 9 CFR 317, 9 CFR 320.1, and 9 CFR 381.175, and the collection of information for Forms 7234-1 and 8822-4 is authorized in OMB Statement 0583-0092.

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

Name and work location contact information of applicants is collected by and expeditor or establishment employee in order to make the necessary follow-up communications. While there is a risk this private information could be shared, there are substantial protections to help ensure that does not occur. LIS enforces encryption, controlled access based on e-Auth, timeout for remote access and system audit logs to ensure that information is handled securely and appropriately. E-authentication is used to identify and control system access to authorized users only, as well as to further limit access to certain processes to an even smaller subset of authorized users. When the user initiates the system, their login credentials and responsibility levels are passed to LIS.

In addition, authorized user login ids are appended to any system records created or updated, allowing administrators to identify the source of a transaction or action.

Also, 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 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.

FSIS system users must pass a Government National Agency Check with Inquiries background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

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 that labels for meat, poultry, and processed egg products are safe for human consumption, 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. LPDD is responsible for checking and verifying that the labels comply with regulation 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 LIS to allow LPDD to run reports for individual submission, summarized data analysis, and management controls. Crystal report is used for data analysis; LIS 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 requests.

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

N/A – LIS does not use commercial 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.

LIS enforces controlled access based on e-Auth, timeout for remote access, and system audit logs to ensure that information is handled in accordance with the above described uses. Multiple levels of access exist based on the authorized user's role and

job function. The level of access restricts the actions that a user can take and the data a user can see. This also helps to ensure that the data is being seen and handled by those who are trained in its use and trained to control unauthorized access.

Mitigation controls are addressed in Section 1.7 above. However, 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 OMB Circular A-130, Appendix III. The security controls in the system will be reviewed when significant modifications are made to the system, but at least every three years.

The e-Authentication identifies the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When the user access LIS, the secure network login credentials are passed to the system via Active Directory.

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 transaction and 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 and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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?

All of the Label decisions are recorded and retained in the LIS database. A Labeling and Consumer Protection Staff reviewer’s decision may be appealed by the applicant. All appeals and appeal decisions are also recorded in the LIS database. Thus the information is retained since the deployment of LIS.

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.

There are no additional risks involved due to retention of data. To mitigate this risk, the system is maintained in an access-controlled facility and on an access-controlled network. In addition, logical access to the application and data is restricted to authorized personnel.

See Section 1.7 above for a description of the controls that have been put in place for LIS.

LIS enforces encryption, controlled access based on e-Auth, timeout for remote access and system audit logs to ensure that 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 information technology. 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 application information is shared as needed with others in FSIS when problems with product (e.g., recall) or other substantive question arises. Information that is shared is product and establishment specific and does not include PII.

In addition, LPDD identifies individuals authorized to:

- access the information system from the external information systems- PBIS and AIIS;
- process, store, and/or transmit organization-controlled information using the external information systems- PBIS and AIIS.

LIS connects with PBIS and AIIS as follows:

Between LIS and PBIS:

The information is shared between the two systems when an LIS user enters the Establishment number for a Domestic food processing location, LIS accesses PBISReader to confirm the Establishment number. Specifically, LIS accesses PBIS. No changes are allowed – read only access is allowed for this connection. No PII data is passed at all between the systems.

Between LIS and AIIS:

The information is shared between the two systems when an LIS user enters the Establishment number for a foreign food processing location, LIS accesses an AIIS database table to confirm the Establishment number. Specifically, LIS accesses AIIS to confirm the Establishment number of foreign entities. No changes are allowed – read only access is allowed for this connection. No PII data is passed at all between the systems.

4.2 How is the information transmitted or disclosed?

The Organization processes and transmits sensitive but unclassified (SBU) and/or classified data that require protection for confidentiality, integrity and availability. During the communication between LIS and PBIS or LIS and AIIS, only LIS access the other system. There is no transmission or disclosure of PII in any form (encrypted or un-encrypted). The information disclosed is just read-only.

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.

The impact of privacy risks on LIS, considering the extent of internal information sharing in Moderate. Even though the PII is stored for LIS, it is never transmitted or disclosed to any other system. The connections LIS – PBIS and LIS – AIIS are passive.

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?

Label Information System does not share any information with organizations external to 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.

Not-applicable as no PII is shared and no information is routinely shared outside of USDA.

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

Not-applicable as no information is shared outside USDA.

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

Not-applicable as no information is shared outside USDA.

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

Yes, it is provided on both the Form 7234-1 and Form 8822-4, according to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is **0583-0092**.

The information provided by the customer will help ensure that labels for meat, poultry, and egg products are safe for human consumption, accurate, and not misleading. The information will also help to protect consumers from any misbranded or economically adulterated meat, poultry, and egg products.

USDA is also authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note) as well as TITLE 5 PART I CHAPTER 3 - 301, and 5 USC 552 - Sec. 552a.

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

Yes, but providing the information is a requirement for access to the system.

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

No.

6.4 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 Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: fsis.foia@usda.gov. Personnel in that division will then forward the request to the USDA agency that they believe is most likely to maintain the records the individual is seeking.

The individual must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; current mailing address and zip code; signature; CCMS case number, if applicable and known; and a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

For more information about how to make a FOIA request, please see http://www.fsis.usda.gov/FOIA/FOIA_Request/index.asp

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

Individuals can contact the LIS System Owner from LPDD Program Area. LPDD contact information is also listed on the LIS website. For label submissions, if the application is still in a pending status, the individual may withdraw the application themselves. If the application is already in a review status, then the individual would need to contact LPDD LIS administrator.

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?

Please refer 7.2 above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy risks are minimized as the addresses collected are generally business and not personal.

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 LIS users are from the LPDD and a few are from USDA Agriculture Marketing Services (AMS). Access is only granted to individuals from these two program areas who are involved in the label submission and approval life cycle process. Access to LIS is strictly controlled and is based on business needs. Plus, user roles are well defined and documented in the SSP. The department-wide e-Authentication process is used for LIS, providing additional protection.

8.2 Will Department contractors have access to the system?

The only department contractors that who access LIS will be from the OCIO areas i.e., technical staff supporting LIS for FSIS and AMS.

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 expert in such matters.

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

USDA Security Awareness and Privacy Training is provided to all users. As a condition of system access, users must successfully complete security training on a regular basis or lose system access rights.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

LIS ATO was granted 4/06/2011.

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

LIS enforces encryption, controlled access based on e-Auth, timeout for remote access and system audit capability. The audit process is carried out only when an incident happens.

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?

The primary risk is that information may be shared inappropriately. These risks are mitigated as noted in 1.7 above. 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 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?

LIS is a major application for FSIS.

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

The single area of concern has been previously addressed by a Plan of Action and Milestone (15486). The technology in question does not raise privacy issues.

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”?

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

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?

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

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

Ms. Lynn Yoder
Patriots Plaza III
355 E. Street, SW, 8-145B
Washington, DC 20024
United States Department of Agriculture

Alicemary Leach – Director, ECIMS
Office of Public Affairs and Consumer Education
United States Department of Agriculture

Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

Janet Stevens – Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: *Rosalyn Murphy-Jenkins* 9-19-12
Rosalyn Murphy-Jenkins Date
Director, LPDD/ System Owner

Agreed: *Elamin Osman* 9-24-12
for Elamin Osman Date
Chief Information Security Officer (CISO)

Agreed: *Janet Stevens* 9/25/12
Janet Stevens Date
Chief Information Officer

Agreed: *Alicemary Leach* 9-25-12
Alicemary Leach Date
Privacy Officer