

# Privacy Impact Assessment

## Laboratory Information Management System (LIMS)

- Version: 2.3
- Date: July 18, 2012
- Prepared for: USDA FSIS Office of Public Health Science (OPHS)





## Privacy Threshold Analysis – LIMS

---

Document Revision and History			
Revision	Date	Author	Comments
2.0	03/07/2012	Mikael Kebede	Initial Draft
2.1	03/14/2012	LIMS Team	Provided comments and updates to Draft
2.2	03/21/2012	Mikael Kebede	Accepted comments and finalized for signature
2.3	7/18/2012	Mark Whitaker	Update based on comments from Privacy Office.

### Abstract

*This document serves as the Privacy Impact Assessment for the Laboratory Information Management System (LIMS). The purpose of LIMS is to enhance FSIS laboratory productivity and to streamline sample data collection, so that FSIS may accomplish its mission of assuring a safe food supply for the Nation's population. This assessment is being done as a result of LIMS Privacy Threshold Analysis (PTA) conducted in February 2012.*

### Overview

LIMS is a client-server application that is owned, maintained, and operated by the Food Safety and Inspection Service (FSIS) Office of Public Health Science (OPHS).

LIMS is a client-server application that provides complete tracking of a sample from the time it is received at the laboratory until the results are reported. LIMS maintains sample tracking that is required under ISO/IEC Standard 17025, so the FSIS may maintain its mission of assuring a safe food supply for the Nation's citizens.

LIMS functions primarily to capture and store data related to food samples that are processed and analyzed in the Field Services Laboratories (FSL). LIMS performs additional functions to maintain laboratory data integrity and to permit data reporting, analysis and availability to authorized users across the FSIS enterprise.

According to the USDA FSIS OPHS LIMS Project Plan, the primary business objectives that LIMS contributes to are as follows:

- Maintain better sample accountability by tracking chain of custody.
- Improve the quality of data by allowing entry of results and other information into a database from the point of capture.
- Eliminate many paper-based and manual processes by implementing electronic forms and automating many routine calculations.
- Automate many data acquisition, processing, and archiving functions.
- Improve information sharing allowing on-line data accessibility to laboratory information.
- Increase security of laboratory results.
- Automate scheduling of equipment maintenance, calibration, and quality assurance checks.
- Maintain reagent and equipment inventories.

LIMS is deployed at three FSLs and each site has the capability to restrict data access to on-site users to ensure closed data system validation. The LIMS application and transaction

database servers are in operation at each of the three FSL sites. Firewalls are deployed to monitor all data traffic flow on the FSIS enterprise network. Virtual Local Area Networks (VLANs) are configured on the network switches at each laboratory site to allow data communication to be segmented between the LIMS desktop clients and specific network resources. Users may utilize portable devices to conduct data entry and analysis functions; furthermore, the connection to the transaction servers is through a secure wireless network. Each laboratory site has an auditing server that performs audits on all transaction servers deployed within the LIMS environment. LIMS also has a Data Analysis and Reporting Environment that managers use to access the network remotely through an unsecure connection to the reporting server. Secure data replication is enforced on all transaction servers between the three laboratory sites using Internet Protocol Security (IPSEC) on a WAN connection. An antivirus server has been deployed within the environment to manage and monitor the security posture of all LIMS systems.

Maximum use is made of bar coding and direct instrument interfacing, where possible, in order to minimize chances for keyboard data entry errors.

LIMS employs two-factor authentication. Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

User Roles determine what users are able to see and what functional permissions they possess. Groups determine the data and LIMS objects that users are able to view.

Roles determine the functional permissions that users have in the LIMS. Different functional permissions have been assigned to different user roles. Users will have at least one role. Users with more than one role will have a Primary Role and that Primary Role will be their default role displayed in the Role text box on the Login Prompt.

LIMS servers are independent systems configured with operating system (OS) and the LIMS application. The database servers are configured with the operating system (OS), relational database management system (RDBMS), and other supporting applications running on a redundant array of independent disks. The Transaction Log files are on separate disk arrays. The disk array maintains an exact mirror of the data of one disk on another disk. The database files, transaction log backup files, and LIMS-associated file storage are also on disk arrays. Back up of data to local hard drives and to secured tapes provides local secondary and archival data storage.

A Data Analysis and Reporting Environment provide an isolated system for managers and analysts to review and examine data. Also, the LIMS pre-log tables store information from samples scheduled and data records provided by PREP, Residue, PHIS, and LSample, respectively.

For some sampling programs and geographic areas, the Performance Based Inspection System (PBIS) generates profile information in order for PREP and Residue to schedule meat,



## Privacy Threshold Analysis – LIMS

---

poultry, and egg products for sampling. Furthermore, PREP and Residue assist in providing data and sample submission for LIMS. Sample request forms are printed and mailed to FSIS sample collection personnel in the field. The samples are collected, questions about the sample are answered on the form, and both are shipped to an FSIS laboratory for analysis.

For some sampling programs and geographic areas, a new Public Health Information System (PHIS) performs the same sampling and scheduling functions as described for PBIS, PREP, and Residue.

Upon arrival at the laboratory, the samples are logged into LIMS, the answers to questions on the form are entered into LSample, and the data are exported to the CONSOL Transaction tables in the FSIS enterprise database. These data also update the LEARN database for view by the sample collectors. Files for samples scheduled and data records are loaded into LIMS pre-log tables from PREP, Residue, PHIS, and LSample.

When sample analysis is complete, the results are entered into LIMS, exported to the CONSOL Transaction tables and LEARN database, and the data are available to be read by the sample collection personnel via LEARN.

LEARN also uses the sample results from LIMS to send results information to the specific Establishment POC and to FSIS personnel (OFO personnel, HQ staff, and other lab personnel). As such, Establishment POC and FSIS Personnel contact information (name and email address) are included in the messages prepared in LIMS and sent out by LEARN.

Certain sample results that may require more immediate regulatory action are made available to identified Agency personnel via email from LIMS.

The LIMS flow diagram is shown below.



## 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 system collects and processes individual's name (first and last) and work phone numbers and work email address information on individuals, as identified in LIMS PTA as Personally Identified Information (PII). The individuals are LIMS users (USDA employees and contractors working on behalf of USDA). When a user is granted access to the LIMS application, a UserID (user account name) is created and maintained.

Name and work contact information is also stored and processed for non-federal personnel who are commercial establishment points of contact (POCs). The POCs information includes names (first and last), work phone numbers, and work e-mail addresses. NOTE: the commercial establishment POCs are not LIMS users and do NOT have access to LIMS.

In addition, the LIMS application maintains information about tests (and the results) conducted on food samples sent to the FSIS Field Services Laboratories (FSL) from commercial establishments.

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

For employees and contractors, the source of their information is directly from the individuals. The information is entered into the LIMS application by a LIMS System Administrator at the time of user account creation.

For individuals from the commercial establishments (i.e., not federal employees or contractors), the source of the information is from the Public Health Information System (PHIS), the Performance-based Inspection System (PBIS) & Sample Analysis Management (SAM) system, which consists of the following components: LEARN, Lsample, PREP, and Residue), which pass the information electronically to LIMS.

For the non-PII information (i.e., test results on food samples), the source of the information is from FSL scientists who conduct the tests and enter the information directly into the LIMS application.

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

With regard to the food sample test activities and results, the information is collected, used, disseminated, and maintained as part of the FSIS mission of assuring a safe food supply (e.g., meat and poultry products) for the Nation's population. This testing helps FSIS and the commercial establishments to determine when food products need to be recalled and the public alerted.

For employees and contractors, their information (first and last name, work phone number, and work email address) is collected, and maintained in associated with their LIMS user account and so that they can (as necessary) receive emails from LIMS.

Establishment POC information is needed for transmission of sample receipt and test result information to commercial establishment management personnel.

Information is also sent to Establishment POC and FSIS personnel (OFO personnel, HQ staff, and other lab personnel) in Biological Information Transfer and Email System (BITES, a component of LIMS) e-mail messages. While LIMS builds the BITES email, it does not actually send out the email to the specified recipients. It puts the email in the FSIS CONSOL database. The email is provided by CONSOL to the FSIS Learn application (which is part of the SAM system). The Learn application actually sends out the BITES email to the Establishment POC and FSIS personnel.

### **1.4 How is the information collected?**

For Federal employees and contractors, the information is initially taken from the individual (new FSIS employee) seeking access to LIMS. LIMS system administrators enter the information at the time of LIMS user account creation.

Commercial establishment POC information is collected and entered into PHIS, PBIS, and SAM and transmitted electronically to LIMS.

For the non-PII information (i.e., test results on food samples), the information is collected by having FSL scientists who conduct the tests enter the information directly into the LIMS application.

### **1.5 How will the information be checked for accuracy?**

For USDA employees and contractors, the data are verified by the individual's manager and LIMS administrator. The user also has a chance to verify the information for accuracy.

For commercial establishment POCs, the information is checked at the source when the data is created (see PHIS, PBIS, and SAM). LIMS System Administrators do not check for accuracy for commercial establishment POC information sent from other applications.

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

Full name of laboratory employees are collected under terms of federal employment.

US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.

The November 18, 2008, amendment to the Executive Order 9397 directs Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unauthorized use.

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

Given the information noted above in Sections 1.1, the risk is that the PII or food sample test results might be disclosed to unauthorized individuals. To mitigate the risks of using this PII, the measures outlined below help mitigate the risk of maintaining this information. As such, this risk is considered to be minimal (or Low).

LIMS System Administrators and general users access the system using unique, authorized accounts. LIMS cannot be accessed without an authorized account that required two-factor authentication (users must possess and insert a USB token when logging in). LIMS cannot be accessed by external users. 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.

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 user accounts (for access to the FSIS issued workstations and FSIS Network environment) and LIMS 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 anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account. In addition, they also have to obtain a LIMS user account to access LIMS. To access LIMS, the user must first login to the FSIS network environment by using their Active Directory account to login to their FSIS issued laptop or a workstation in the access controlled Lab. As a result, their secure network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. The LIMS user account is used to login to LIMS. A user must use their password and a valid token to login. When a user accesses LIMS, there are LIMS 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.

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 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 expert 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.

With regard to the food sample test activities and results, the information is collected, used, disseminated, and maintained as part of the FSIS mission of assuring a safe food supply

(e.g., meat and poultry products) for the Nation's population. This testing helps FSIS and the commercial establishments to determine when food products need to be recalled and the public alerted.

For employees and contractors, their information (first and last name, work phone number, and work email address) is collected, and maintained in associated with their LIMS user account and so that they can (as necessary) receive emails from LIMS.

Establishment POC information is needed for transmission of sample receipt and test result information to commercial establishment management personnel.

Information is also sent to FSIS personnel (OFO personnel, HQ staff [e.g., FSIS Assistant Administrators, Data Analysts, Directors, Economists, Press Officers, Risk Analysts, etc.], and other lab personnel) in Biological Information Transfer and Email System (BITES, a component of LIMS) e-mail messages. As noted above in Section 1.3, LIMS does not actually send the BITES email.

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

For LIMS user (USDA employees and contractors), their name is used to create (produce) a LIMS user account (UserID). This information is not analyzed.

Commercial establishment POC information is not analyzed.

For the food sample information, the food samples are tested and analyzed in the labs but external to LIMS using various testing tools and systems. The test activities and results are entered in to LIMS by the FSL scientists.

Data may be directly queried from the LIMS application (e.g., through the application interface or directly from the database tables). This includes a list of current LIMS users and their actions. In addition, reports can be run to show food sample testing activities and results.

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

LIMS does not use commercially 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.**

Given the information noted above in Sections 1.1, the risk is that the PII or food sample test results might be disclosed to unauthorized individuals. To mitigate the risks of using this PII, the measures outlined below help mitigate the risk of maintaining this information. As such, this risk is considered to be minimal (or Low).

See Section 1.7 above for a description of the controls that have been put in place for LIMS and the FSIS environment.

## **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?**

The information is retained until all related laboratory records are archived. LIMS Administrators review and disable accounts.

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA).

FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

### **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 are retained and how those risks are mitigated.**

There is minimal privacy risk with the length of time data are retained.

Given the information noted above in Sections 1.1, the risk is that the PII or food sample test results might be disclosed to unauthorized individuals. To mitigate the risks of using this PII, the measures outlined below help mitigate the risk of maintaining this information. As such, this risk is considered to be minimal (or Low).

See Section 1.7 above for a description of the controls that have been put in place for LIMS and the FSIS environment.

## **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?**

Information is shared with internal organizations, including OFO, HQ staff (e.g., FSIS Assistant Administrators, Data Analysts, Directors, Economists, Press Officers, Risk Analysts, etc.), and lab personnel involved with or who must take action as a result of in pathogen testing results, particularly as they relate to possible control measures or recalls.

**4.2 How is the information transmitted or disclosed?**

Information is transmitted via BITES e-mail messages and disclosed in BITES e-mail messages and LIMS reports. While LIMS builds the BITES email, it does not actually send out the email to the specified recipients. It puts the email in the FSIS CONSOL database. The email is provided by CONSOL to the FSIS Learn application (which is part of the SAM system). The Learn application actually sends out the BITES email to the Establishment POC and FSIS personnel.

**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.**

There is minimal privacy risk with internal sharing the USDA employee, contractor, and commercial establishment POCs first and last names, work phone numbers, and work email addresses.

This is because of the access control measures that are discussed above in Section 1.7. LIMS is maintained in access controlled government buildings, users must successfully login to a FSIS issued workstation/laptop and then successfully login to the FSIS network before the LIMS application can be launched, access to the LIMS system is limited to authorized USDA Employees and contractors, two-factor authentication is used to control access, and there are less than ten (10) LIMS System Administrators.

Furthermore, authorized employees 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. The level of access associated with a LIMS user's role restricts the data that may be seen and the degree to which data may be modified by the user.

## **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?**

Test results for a specific commercial establishment are shared with the POC for that specific commercial establishment so that the commercial establishment can either release product into commerce or take the appropriate control measures, up to and including recall.

However, PII information is not routinely shared with external organizations.

If necessary, information may be disclosed to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to

FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

**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.**

Under routine circumstances, LIMS does not share PII outside the Department. However, routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised. As such LIMS requires a SORN. The option of putting LIMS under an umbrella SORN is being explored.

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

Should LIMS information need to be shared with NARA, Congress, or Department of Justice, standard FSIS guidelines for providing information to such organizations will be followed.

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

As under normal operating circumstances, employee information is not shared externally; in fact, such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

## 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, for employees, their information (name) is collected at the point of hiring. For contractors, the information is provided when applying for FSIS credentials (e.g., a badge).

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information. As such a SORN is required. The option of putting LIMS under an umbrella SORN is being explored.

Contact information provided by establishment personnel is collected by other systems and is addressed by the PIAs for those systems: PHIS, PBIS, and SAM.

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

Yes. However, the information is required in order to gain access to the FSIS and LIMS environments. If the person (potential employee or contractor) refuses to provide the information they will not be given access to the FSIS or LIMS environments. As such LIMS requires a SORN. The option of putting LIMS under an umbrella SORN is being explored.

Contact information provided by Commercial Establishment POC personnel is collected by other systems and is addressed by the PIAs for those systems: PHIS, PBIS, and SAM.

### **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. LIMS requires a SORN. The option of putting LIMS under an umbrella SORN is being explored.

Contact information provided by establishment personnel is collected by other systems and is addressed by the PIAs for those systems: PHIS, PBIS, and SAM.

**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.**

In accordance with Directive 8010.12, if personal information is obtained from an FSIS employee or contractor, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information. As such LIMS requires a SORN. The option of putting LIMS under an umbrella SORN is being explored.

## **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?**

The user (USDA employee/contractor) name is part of the authentication and LIMS access process. If the user name is not correct, access will not be provided. Users can contact the FSIS Service Desk at 1-(800) 473-9135 to begin the correction process.

Individuals seeking notification of and access to any record contained in LIMS may submit a request in writing to the Headquarters or component's FOIA officer, whose contact information can be found at <http://www.da.usda.gov/foia.htm> under "contacts".

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

See 7.1 above.

**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. The individual's acknowledgement of the Privacy Act Notice signifies the individual's consent to the use of the information. The purpose, use, and authorization for collection of information are described in the Privacy Act Notice.

For non-federal personnel, refer to the PIA at the source of information (PHIS, PBIS, SAM).

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

See 7.1 above.

**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?**

To gain access to the system a user must first have an account on the FSIS Active Directory. In addition, a user must have a LIMS user account (with dual factor authentication – a user must possess a LIMS USB token) and a role with the LIMS application. The LIMS System Security Plan (SSP) documents that LIMS administrators establish, activate, modify, review, and disable accounts. Documentation that describes the LIMS Users roles is

maintained on the LIMS SharePoint repository. LIMS users are assigned specific roles based on the privileges they need per their job and in accordance with applicable policy.

System Administrators and users of the system will have access. Authorized employees 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.

### **8.2 Will Department contractors have access to the system?**

Yes. Contractors authorized to access LIMS 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?**

Annual, recurring computer security awareness training is practiced and conducted through the Office of the Chief Information Officer. If users do not take and pass this required training, their access to the FSIS environment, its network and applications, are revoked.

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

Yes, the ATO was granted on July 14, 2010, and is scheduled to expire on July 14, 2013.

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

Applying security patches and hot-fixes, continuous monitoring (e.g., vulnerability scanners are run on the LIMS servers), checking the national vulnerability database, following

and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

All events are logged in the underlying SQL database. Authorized user login identifiers are appended to event log 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. Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. An access agreement describes prohibited activities (such as browsing). Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

In addition to auditing measures, LIMS has multiple physical and logical safeguards to prevent the misuse of data. The systems are maintained in access controlled facilities, they are only access by a limited set of authorized users, the application is not accessible by the public, logging onto the application requires two-factor authentication. These safeguards are continuously monitored as part of the C&A and Annual Assessment process.

### **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 risks are that the USDA employee, contractor, or commercial establishment POC information (name, work phone number, and work email address), may be incorrect or that it may be disclosed to unauthorized individuals. These risks are mitigated by the following safeguards.

LIMS uses the access control mechanisms discussed in Section 1.7 (above) to ensure that information is handled in accordance with the above described uses.

In addition, LIMS is under an ATO and goes through Annual Self Assessment to comply with FISMA guidelines to ensure continuous security. Moreover, LIMS systems are continuously monitored by Security Operation Center (SOC) to ensure that information is handled in accordance with the above described uses.

Finally, the overall security of LIMS servers and its network infrastructure is continuously monitored by the FSIS Security Operation Center (SOC) via various automated monitoring tools.

## 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?

LIMS is a non-major application.

LIMS is a client-server application that provides complete tracking of a sample from the time it is received at the laboratory until the results are reported. LIMS functions primarily to capture and store data related to samples that are processed and analyzed in the Field Services Laboratories (FSL). LIMS performs additional functions to maintain laboratory data integrity and to permit data reporting, analysis and availability to authorized users.

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

Although minimal, the inclusion of USDA employee, contractor, or commercial establishment POC information (name, work phone number, and work email address) in BITES e-mails may raise privacy concerns. While LIMS builds the BITES email, it does not actually send out the email to the specified recipients. It puts the email in the FSIS CONSOL database. The email is provided by CONSOL to the FSIS Learn application (which is part of the SAM system). The LEARN application actually sends out the BITES email to the Establishment POC and FSIS personnel.

## 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 team.

**10.2 What is the specific purpose of the agency’s use of 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party websites**

**and/or applications, discuss the privacy risks identified and how they were mitigated.**

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



Privacy Threshold Analysis – LIMS

**Responsible Officials**

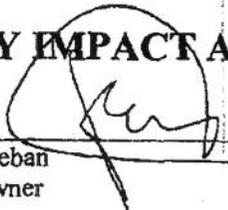
Emilio Esteban  
Office of Public Health Science (OPHS)  
Food Safety and Inspection Service (FSIS)  
United States Department of Agriculture

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

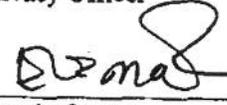
**Elamin Osman** – Chief Information Security Officer  
Office of the Chief Information Officer  
Office of the Administrator  
United States Department of Agriculture

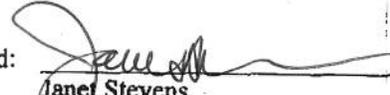
**Janet Stevens** – Chief Information Officer  
Office of the Chief Information Officer  
Office of the Administrator  
United States Department of Agriculture

**PRIVACY IMPACT ASSESSMENT APPROVALS**

Agreed:  \_\_\_\_\_ Date 7/18/12  
Emilio Esteban  
System Owner

Agreed:  \_\_\_\_\_ Date 7-26-12  
Alicemary Leach  
Privacy Officer

Agreed:  \_\_\_\_\_ Date 8/23/12  
Elamin Osman  
Chief Information Security Officer (CISO)

Agreed:  \_\_\_\_\_ Date 8/24/12  
Janet Stevens  
Chief Information Officer