Privacy Impact Assessment

Laboratory Information Management System (LIMS)

- Version: 7.2
- Date: August 26, 2020
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Laboratory Information Management System (LIMS)

August 26, 2020

Contact Point
William Shaw – System Owner
FSIS/OPHS
202-720-6246

Reviewing Official
Emmanuel Olufotebi
Privacy Office
United States Department of Agriculture

Revision History*

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
2.4	5/30/2013	Paul Kuscher	New Document template and new PIA Document
2.5	2/21/14	Paul Kuscher	Annual Update
2.6	09/08/14	Paul Kuscher	Annual Update
3.0	03/03/2016	Erik Nudo	Annual Update
3.1	6/14/2016	Erik Nudo	Review and Signature from System Owner
3.2	6/27/2016	Erik Nudo	Review and Signature from CISO
3.3	6/27/2016	Erik Nudo	Review and Signature from CIO
3.4	7/15/2016	Erik Nudo	Update to latest template based on comments from Privacy Office
4.0	7/20/2016	Erik Nudo	Incorporate FSIS Privacy comments. Signature from Privacy and Finalize.
4.1	12/20/16	Tope Ayodeji	Annual Update for FY17 A&A
4.2	1/13/2017	Frank Niagro	Annual Review and Edit
5.0	3/27/17	Tope Ayodeji	Annual Update
5.1	11/27/17	Tope Ayodeji	Annual Update
5.2	12/29/2017	Frank Niagro	Annual Update
6.0	05/23/2018	Kathryn Stuart	Finalize FY18 Annual Update

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
6.1	10/05/2018	Kathryn Stuart	FY19 Annual Review and Preparation for ATO Renewal
6.2	11/05/2018	Frank Niagro	Consolidated updates from LIMS stakeholders for FY19 review
6.3	2/12/2019	Kathryn Stuart	Finalized for SO signature and Privacy Office Review
6.4	4/22/2019	Kathryn Stuart	Updated with new LIMS Acting SO Contact Information
6.5	5/14/2019	Kathryn Stuart	Updated with Privacy Office point of contact who reviewed and signed
7.0	5/23/2019	Kathryn Stuart	Finalized document for FY19 upon receipt of final CIO signature.
7.1	4/30/2020	Kathryn Stuart	FY20 Annual Review and Update
7.2	8/26/2020	Erik Nudo	Finalize for FY20

***NOTE:** *During Annual Assessment, the System Owner and/or Information System Security Officer (ISSO) Representative reviews this Privacy Impact Assessment (PIA). A Revision number is identified in the table to represent this annual review, although no document signatures are required unless significant system/organizational document changes are involved.*

Abstract

The name of this system is the Laboratory Information Management System (LIMS). LIMS functions primarily to capture, store, process, and report data related to samples that are processed and analyzed in the Field Services Laboratories (FSL). Based on the results of the Privacy Threshold Analysis, this PIA is being conducted.

Overview

LIMS is an "umbrella" entity recorded in CSAM and is comprised of more than 1000 unique information technology systems that support FSIS laboratory operations, including the testing of various food products collected under agency sampling programs. Those IT systems include laboratory equipment and software applications managed funded by both the Lab GSS and WGS Investments. Most lab equipment (incubators, freezers, pipettors, analytical balances, etc.) do not store or process PII. Those lab systems that do process or store PII utilize various mechanisms for identifying, authenticating, and authorizing users.

- The legal authority to operate the program or system is provided by the signed ATO letter dated 07/08/2019.
- The various systems that process or store PII are located at one of five physical sites listed below and summarized in the following table:

Location Name	Abbreviation	Location
• Eastern Laboratory	EL	Athens, GA
• Midwestern Laboratory	MWL	St. Louis, MO
• Western Laboratory	WL	Albany, CA
• Primary Enterprise Data Center	EDC (P)	Kansas City, MO
• Backup Enterprise Data Center	EDC (B)	St. Louis, MO

Item Name	Location	Purpose, Transactions, and Type of PII
LabWare Application	EL, MWL, &WL	Principal, compliant (21 CFR 11) electronic record system for FSIS laboratory operations, including the entry, processing, storage, and reporting of laboratory sample status and testing results. Includes integrated functions for equipment maintenance, inventory, statistical quality control charting, and other functions that support reportable test results and accreditation of the FSIS laboratories under ISO 17025. User PII for identification, authentication, and authorization in the application. Names and e-mail addresses for federal employees and contractors, commercial establishment contact

		personnel, and state public health contacts. Images of handwritten signatures and initials of personnel.
LabWare Database	EL, MWL, WL, EDC (P), & EDC (B)	Replication of transactional data from each FSIS lab site for business continuity, disaster recovery, and for centralized interconnection with other agency data systems. User PII for identification, authentication, and authorization in the application. Names and e-mail addresses for federal employees and contractors, commercial establishment contact personnel, and state public health contacts. Images of handwritten signatures and initials of personnel.
BITES Messages	EDC (P)	Alert notifications of certain testing results for certain project samples that are sent to FSIS employees via email. Name and e-mail address of FSIS personnel. Name and phone number of establishment contact person.
LIMS Reporting Server:	EL	Preconfigured, parameterized reports containing data from LIMS tables. Used for management of laboratory operations and to provide access to laboratory data for designated HQ personnel. User PII for identification, authentication, and authorization in the application. Names and e-mail addresses for federal employees and contractors, commercial establishment contact personnel, and state public health contacts.
LIMS Direct:	EDC (P)	Preconfigured, parameterized reports containing data from LIMS Direct tables. Used by agency personnel to view testing results for samples submitted to FSIS labs. User PII for identification, authentication, and authorization in the application. Names and e-mail addresses for federal employees and contractors, commercial establishment contact personnel, and state public health contacts.
LIMS Direct Plant E-Mails	The Internet	Email notifications to commercial establishments from which collected samples have been received at a FSIS lab and certain testing results when those results are released. These notifications are also sent to some state agency personnel. Names and e-mail addresses of establishment and state contact personnel.
BioNumerics	EL	Normalization and annotation of electrophoretic gel images, uploading of images to PulseNet

		national database (CDC), and downloading of PFGE pattern names. Uploading of DNA sequencing data and downloading of genome characterization records. No PII.
CheckPoint (ViewPoint)	EL, MWL, & WL	Monitoring of temperature in laboratory equipment (incubators, refrigerators, incubators, etc.) and temperature and humidity in laboratory rooms. Latest application version is named "ViewPoint. User PII for identification, authentication, and authorization in the application.
CISPro database (archived)	EL, MWL, & WL	Archived system for management of chemical and consumable laboratory supply inventories. Management of chemical waste disposal. User PII for identification, authentication, and authorization in the application when the systems were active.
ROPS database (archived)	EL, MWL, & WL	Archived system for management of laboratory supply and equipment requisitioning and ordering activities, including tracking of budget utilization. User PII for identification, authentication, and authorization in the application when the systems were active.
CLC Genomics	EL & MWL	Bioinformatic analysis of bacterial genome sequence data. No PII.
Numerous Windows-based Lab Instruments	EL, MWL, & WL	Analysis of laboratory samples. No PII.
Numerous Linux-based computers	EL & MWL	Bioinformatic analysis of bacterial genome sequence data. No PII.
LRN Messenger Server	EL	Testing results and data concerning LRN laboratory testing. User PII for identification, authentication, and authorization in the application.
Containment Lab Environmental Control and Waste Management System	EL	SCADA functions for biocontainment laboratory environmental and waste processing systems. No PII.
PEPRLab	LQAS	Oversight of Pasteurized Egg Product Recognized Laboratory (PEPRLab) program. Participating laboratories are private laboratories providing egg product testing for federally inspected egg product establishments. PII include full name, work address, work telephone

		number, work e-mail address of lab contact personnel.
ALP	LQAS	Oversight of voluntary Accredited Laboratory Program for non-federal laboratories that analyze meat and poultry products for food chemistry and residues. Provide audits, proficiency testing samples, and certification to participating laboratories. PII include full name, work address, work telephone number, work e-mail address of lab contact personnel.
CIS	LQAS	Oversight of Cooperative Interstate Shipment (CIS) Program participating laboratories (state and/or private laboratories) providing audits and "same as" evaluations of QA programs and methods. PII include full name, work address, work telephone number, work e-mail address of lab contact personnel.
MPI	LQAS	Oversight of State Meat and Poultry Inspection (MPI) system participating laboratories (state and/or private laboratories) providing audits and "at least equal to" evaluations of QA programs and methods. PII include full name, work address, work telephone number, work e-mail address of lab contact personnel.
Lab Photocopiers and Printers with Non-Volative Memory	EL, MWL, WL, LQAS, FERN, EALS	Making copies of paper documents, scanning paper documents, faxing paper documents. PII stored on equipment may include Full Name; home address; SSN; home telephone number; emergency contact phone number; name, address, telephone number of emergency contact individual; employee payroll information; electronic image of face; electronic image of driver's license or other picture ID; electronic image of handwritten signature or initials; names, addresses, and telephone numbers of family members; names, addresses, and telephone numbers of personal or professional acquaintances; other PII from any paper document that has been scanned or copied on the device.

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 name (first and last), work phone numbers, and work e-mail address information on individuals, as identified in LIMS PTA as 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, state agency, and testing laboratory POCs. The POCs information includes: name (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 LabWare application maintains information about tests (and the results) conducted on food samples sent to the FSIS 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 LabWare application by a LIMS System Administrator at the time of user account creation.

For individuals from the commercial establishments, state contacts, and labs (i.e., not federal employees or contractors), the source of the information is from the PHIS, paper records, or e-mail content.

ALP, PEPRLab, CIS, and MPI subsystem information is provided in applications to those various programs.

For the non-PII information (i.e., test results on food samples), the sources of the information are FSL scientists who conduct the tests and enter the information directly into the LIMS application and laboratory instruments via direct data feeds.

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

Regarding 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 and state agency POC information is needed for transmission of sample receipt and test result information to commercial establishment management personnel from LIMS-Direct.

Information is also sent to FSIS personnel (OFO personnel, HQ staff, and other lab personnel) in Biological Information Transfer and E-mail System (BITES, a component of LIMS) e-mail messages. Establishment POC receive sample result information via e-mails sent by LIMS Direct.

ALP, PEPRLab, CIS, and MPI subsystem information is collected as part of a lab's application to the respective program. The data are needed for program management and to contact the lab, if needed.

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 and transmitted electronically to LIMS. State contact information is entered into LIMS by LIMS managers, based on e-mail requests from state agencies

OMB registered FSIS data collection Forms to gather the information and to receive updates as required by the PEPRLab program SOP.

For the non-PII information (i.e., test results on food samples), the information is collected by having FSL scientists, who conduct the tests, and 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 are created or edited (see PHIS). LIMS System Administrators do not check for accuracy for commercial establishment or state agency POC information sent from other applications.

ALP, PEPRLab, CIS, and MPI subsystem information is entered based on the application filed by the applying lab. The lab points of contact get a chance to review their info periodically (twice a year prior to sending out the PT samples for example). This is done through e-mail

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.

Given the information noted above in Section 1.1, the risk is to the PII. 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. Most subsystems of LIMS (e.g., the LabWare client-server application) cannot be accessed without an authorized account that requires two-factor authentication. However, other subsystems only require a USDA domain account (e.g., Reporting Server) or physical access to a lab instrument and knowledge of the admin account password). For the LabWare application, users must possess and insert a USB token when logging in and the token serial number must have been configured for their user account. LIMS cannot be accessed by external users. There are anonymous user accounts for most of the subsystems (lab instruments) in the LIMS. 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 may exist in a subsystem (e.g., the LabWare application, 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 e-mail account and an FSIS user account. In addition, they also must obtain a user account to access the individual subsystems of LIMS. To access a networked subsystem of LIMS, the user must first log into the FSIS network environment by using either their Active Directory account or a shared-password Active Directory account to log into their FSIS issued laptop or a workstation. As a result, their secure network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly.

Risk is further mitigated as 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).

In the LabWare application, authorized user login identifiers are appended to any system records created or updated through the graphical interface, along with the date and time of the record creation or change. This occurs for about 80% of database transactions. 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.

Regarding the food sample test activities and results, the information is collected, used, disseminated, and maintained as part of the FSIS mission. 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 is collected, and maintained in association with their LIMS subsystem user accounts. This allows employees to receive e-mails from LIMS.

Establishment and state agency POC information is needed for transmission of sample receipt and test result information to commercial establishment management personnel by LIMS Direct.

Information is also sent to FSIS personnel (OFO personnel, HQ staff [e.g., FSIS Assistant Administrators, Directors, Risk Analysts, etc.], and other lab personnel) in BITES e-mail messages.

Information concerning the ALP, PEPRLab, CIS, and MPI programs are used to provide oversight of the various system participating laboratories (state and/or private laboratories) providing audits and "at least equal to" evaluations of QA programs and methods.

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

For the LIMS user (USDA employees and contractors), their name is used to create a LIMS user account. 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 various LIMS subsystem databases (e.g., through the application interface or directly from the database tables). This includes a list of current LIMS subsystem users (and their actions for the LabWare application). 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. Some accredited lab POC PII is posted on FSIS website by OIEA, FSAB

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.

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.

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 kept for 5 years, or the lifetime of the record, whichever is longer.

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

Yes. 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), unless superseded by Lab Management System documents (see LW-0003). 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 kept for 5 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.

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

Because of existing controls, the risk of unauthorized access or inappropriate use of information is considered to be minimal or low. This does not change based on the

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

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?

Sample testing 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, pathogen testing results, particularly as they relate to possible control measures or recalls. Some accredited lab POC PII information is shared with OIEA, FSAB, for posting on the FSIS website. PII for most subsystems is not shared unless requested by FSIS management.

4.2 How is the information transmitted or disclosed?

Information is transmitted via BITES e-mail messages, disclosed in BITES e-mail messages, and LIMS reports. BITES e-mail is encrypted via FSIS VPN. Some PII is transmitted via Plant E-Mails from LIMS Direct, which are sent in plain text.

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 or state agency POCs first and last names, work phone numbers, and work e-mail 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 log in to an FSIS issued workstation/laptop, and then successfully log in to the FSIS network, before the LabWare 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 to the LabWare application, and there are fewer than fifty (50) LIMS subsystem 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 some LIMS subsystem 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?

Some accredited lab POC PII is posted on FSIS website by OIEA, FSAB. Some FSIS lab POC PII is shared with the US Centers for Disease Control and Prevention via the Laboratory Response Network application.

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.

Some accredited lab POC PII is posted on FSIS website by OIEA, FSAB. A SORN does not exist for LIMS but is in the process of being created.

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

Should LIMS information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law. Some accredited lab POC PII is posted on FSIS website by OIEA, FSAB.

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

As long as employee PII data are transmitted externally, there is the risk that the data may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed, except that plant e-mail notifications containing PII are sent in plain text across the Internet

Some accredited lab POC PII is posted on FSIS website by OIEA, FSAB.

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.

LIMS requires a SORN and is currently in the process of developing one.

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

Plant vendors are provided notification during business agreement processes. The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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

No. The information is required 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.

Contact information provided by Commercial Establishment POC personnel is collected by other systems and is addressed by the PIAs for those systems: PHIS, State agency and lab personnel do not have the right to decline to provide the information.

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

No. Contact information provided by establishment personnel is collected by other systems and is addressed by the PIAs for those systems: PHIS, State agency and lab personnel are not provided 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 user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

As lab users enter the data themselves or see the data in the system, there is no lack of awareness, and thus, no risk. However, there is no awareness for non-FSIS persons.

Failure to have this information can lead to greater risks in FSIS being unable to respond to an incident.

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 and wish to obtain a copy 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@fsis.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?

The individual wishing to correct inaccurate or erroneous information should contact the system owner.

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

Individuals have not been notified.

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

Not applicable, as redress is provided. See 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.

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 many of the subsystems a user must first have an account in the USDA Active Directory. In addition, to access the LabWare application 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 LabWare application. 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. In many of the subsystems, roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access may exist depending on the subsystem, 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 OCIO. If users do not take and pass this required training, their access to the FSIS environment, its network and applications, are revoked. Training is not provided to all LIMS contractors.

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

Yes, the ATO was granted on July 08, 2019.

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.

Most of the LIMS subsystems do not provide unambiguous, user-specific authentication mechanisms or auditing. All events in the LabWare application 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, but only for database transactions that are executed through the LabWare application graphical interface. 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 applications are not accessible by the public. Logging onto the LabWare application requires two-factor authentication. These safeguards are continuously monitored as part of the SA&A 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, state agency, laboratory, or commercial establishment POC information, 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 to ensure 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, many LIMS subsystems are continuously monitored by Security Operation Center (SOC) to ensure 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 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?

The LIMS is an "umbrella" entity recorded in CSAM and is comprised of more than 1000 unique information technology systems that support FSIS laboratory operations, including the testing of various food products collected under agency sampling programs. LabWare 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. LabWare functions primarily to capture and store data related to samples that are processed and analyzed in the FSL. LabWare 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, information in BITES e-mails may raise privacy concerns. However, this information is transmitted as encrypted e-mail over the FSIS VPN, mitigating that concern. However, LIMS Direct plant e-mails are sent in plain text and provide no safeguards for information.

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

William Shaw
System Owner
1400 Independence Ave., SW
Washington, DC 20250

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

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

Emmanuel Olufotebi
Privacy Office
Room 1170, South Building
Washington, DC 20250

Approval Signatures

Barring any major changes, no signatures required until ATO expires on 7/8/2022.