Privacy Impact Assessment

Public Health Information System (PHIS)

- Version: 11.0
- Date: May 25, 2021
- Prepared for: FSIS

United States Department of Agriculture

Privacy Impact Assessment for the

Public Health Information System (PHIS)

February 25, 2021

Contact Point
Carl A. Mayes
USDA/FSIS/OA/OCIO
202-720-0294

Reviewing Official

FSIS Privacy Office
(202) 205-0144
United States Department of Agriculture

Revision History*

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
3.0	3/12/2014	Marie T. Penninger	Updated template/Reviewed PIA/Updated document per Privacy Documentation Checklist/ATO update
4.0	8/12/2014	Marie T. Penninger	Annual Update
5.0	10/31/2014	Marie T. Penninger	Annual Assessment FY2015 Update
6.0	02/24/2016	Marie T. Penninger	Annual Assessment FY2016 Update
6.1	11/01/2016	Marie T. Penninger	ATO Update
8.0	10/25/2017	Marie T. Penninger	Annual Assessment FY2018 Update
8.1	02/01/2018	Marie T. Penninger	Completion of Annual Assessment
8.2	12/06/2018	Marie T. Penninger	Privacy Update for inclusion of SCORE
9.0	07/17/2019	Marie T. Penninger	Annual Assessment FY2019
9.1	09/03/2019	Marie T. Penninger	Prepare for Assessment FY2020
10.0	02/13/2020	Marie T. Penninger	Obtain Signatures for ATO
11.0	05/25/2021	Marie T. Penninger	CY21 Annual Assessment

Abstract

This document serves as the Privacy Impact Assessment (PIA) for the United States Department of Agriculture (USDA) Public Health Information System (PHIS). The purpose of the system is to collect, consolidate, and analyze detailed information regarding regulatory compliance verification activities conducted by inspectors at official establishments, official import establishments, and registered facilities. This assessment is being done in conjunction with the PHIS Privacy Threshold Analysis conducted in February 2021 and reviewed annually.

Overview

PHIS collects detailed information regarding regulatory compliance verification activities conducted by FSIS inspectors at official establishments, official import establishments, and registered facilities. PHIS captures more establishment and facility data, and identifies areas that require Agency attention. Additionally, PHIS supports documentation of appeals to inspection decisions, scheduling and documentation of FSAs, and the ability to identify and notify suppliers of beef products that have tested positive for E. coli O157:H7. It manages inspection assignments and employee assignments to roles and establishments.

The PHIS sample scheduler enables the creation and modification of sampling projects. It applies business rules and risk-based algorithms for sample selection and output reports of scheduled samples.

PHIS automates import processes for receiving, verifying, and exchanging information for shipments and products that either were manual processes or performed by AIIS.

PHIS provides the capability to mine and analyze inspection, surveillance and investigative data, predict hazards and vulnerabilities. It communicates or reports analysis results, and target resources to prevent or mitigate the risk of food borne illness and threats to the food supply.

The SCORE module within PHIS is the tool for surveillance and management of consumer complaints and outbreak investigations. The module helps to support the epidemiologists in the OPHS Applied Epidemiology Staff to rapidly identify foodborne issues, communicate with consumers and collaborate with internal and external partners to respond. During time sensitive events such as recalls and outbreaks, it is essential to the Agency for these systems to be operational 24/7 and this is what the integration with PHIS accomplishes.

PHIS shares information with the Laboratory Information Management System (LIMS). Information is written to the LIMS database tables from the PHIS transactional database to be used by other systems including the Data Warehouse GSS. The FSIS data warehouse provides a source of legacy system data and analysis of inspection, audit, and assessment outcomes, and manages data from VetNet and PulseNet.

PHIS provides external interfaces to electronic certification systems maintained by the governments of New Zealand, Australia, and The Netherlands using the United Nations Centre

for Trade Facilitation and Electronic Business (UN/CEFACT) electronic Certificate (eCert) data exchange standard. For other countries, PHIS has the capability to support electronic document warehousing services, such as the Electronic Trade Document Exchange (eTDE) service, which is supported by USDA's Agricultural Marketing Service (AMS) to obtain export health certificates as a temporary solution until foreign governments have implemented UN/CEFACT eCert.

The legal authority to operate the program or system is provided by the signed ATO letter dated 03/17/2020.

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?

PHIS collects, uses, disseminates or maintains the following information: from USDA/FSIS personnel, it collects the users' and the supervisors' first and last names, titles, duty stations and business contact information, including email addresses, the users' assigned PHIS role(s) and e-authentication numbers. It also collects from the USDA/FSIS user their profile data from the National Finance Center, including district assignment, job title, hire dates organizational level pay plan and locality and pay code, and social security numbers (SSN), which the system stores in encrypted format. From the Other Users (Industry and non-USDA government users), PHIS collects, in addition to their names, the identity of the entity, the business contact information, including email addresses, and any unique business identifiers, such as tax identification numbers. The system also collects the names and contact information of non-users as well as complaint details in the case of SCORE which may include medical symptoms and treatment. These details are entered by an authorized PHIS user.

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

Establishment data is provided to FSIS by designated establishment personnel, exporters, and importers. Data from other information technology (IT) systems include the Department of Homeland Security (DHS)/U.S. Custom and Border Protection (CBP) Automated Commercial Environment (ACE) import application data, which is fed to PHIS for import inspection activity, as is the Australian, New Zealand and The Netherlands eCert data, and user account information from the USDA e-Authentication system. Complete employee profile data is obtained from bi-weekly data feeds from the National Finance Center (NFC). Consumer, health care or public health professionals acting on behalf of a consumer provide the data for SCORE. Information received from these sources are manually entered into the system by an authorized user or through a web service that facilitates an import function from Hotline.

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

The USDA/FSIS personnel's information is used for assignment scheduling, to determine role-based access controls, verify employment status, and for records retrieval. The information about Other Users is used for contact, shipping and records retrieval purposes. The information about non-users whose names are entered by authorized users is used for contact purposes. SCORE information is collected to assist with trace-back

or trace-forward investigations to identify product disposition and origin of hazards related to consumer complaints associated with FSIS regulated products.

1.4 How is the information collected?

Sources of this information are the official agency forms (on-line PHIS screens or actual paper form, when applicable) provided to the establishment or business entity acting on behalf of the establishment, legacy data previously provided by these entities and stored in FSIS applications, and the comments made by FSIS reviewers of those forms. Additionally, data is also collected by inspection personnel receiving verbal input or reviewing establishment documents as part of their routine duties. SCORE information is collected directly by USDA/FSIS employees.

Data is provided to PHIS import modules through system interfaces, such as DHS/CBP's ACE System and the Australian, New Zealand, The Netherlands, Chile and Canada eCert systems.

1.5 How will the information be checked for accuracy?

Inspection and district office personnel are required to update and maintain establishment profile data stored in PHIS, and establishment personnel have the ability and responsibility to review this information for accuracy. FSIS Office of Data Integration and Food Protection (ODIFP) also checks for the accuracy of information within PHIS. ODIFP is responsible for coordinating all of the Agency's data collection, analysis, and integration activities across program areas. ODIFP closely collaborates with other offices within FSIS to ensure adherence to emergency management policies, food defense directives, and the consistency and quality of data analyses.

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.

The information being collected includes individual names, establishment name and address. Privacy risks are minimized as the addresses, including email addresses, collected are business and not personal contact information. Access to data is strictly controlled. Access is granted through the USDA-approved secure single sign-on application (e-Auth – Level 2 Access), and authorization within PHIS is role-based to ensure least privileges.

PHIS cannot be accessed without an authorized account. PHIS System Administrators and general users access the system using unique, authorized accounts. This includes federal employees, as well as users from industry and state meat and poultry inspection programs. There are no anonymous, or guest, user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those 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.

PHIS utilizes firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for IT. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act, subsection e[9], and OMB Circular A-108. All of the security controls in the system are reviewed annually or when significant modifications are made and re-authorization every three years. The System Security Plan (SSP), and a subset of these controls, is also reviewed annually. PHIS role-based security is used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system.

The USDA e-Authentication process is used to login to PHIS. When a user accesses PHIS, there are PHIS specific user roles that restrict access. Also, FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. Regular, recurring security training is conducted through the Office of the Chief Information Officer (OCIO).

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 recorded in the system. Any contractors who may be authorized to access the system, such as software developers, are governed by contracts identifying rules of behavior for USDA, FSIS systems, and security. Contracts are reviewed upon renewal by management and contract personnel experts.

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.

PHIS integrates data from all agency systems and program areas for use as a tool in making the most informed decisions about inspections, sampling, policy and other food safety activities to protect public health.

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

Commercial reporting software tools are used to design and generate reports for data analysis. PHIS has the capability to run internal, preprogrammed reports, such as trend reports and management controls for audit purposes, as well as ad-hoc reports in response to specific events and congressional requests. These reports are created and maintained by the PHIS users and FSIS' Office of Data Integration and Food Protection, Data Analysis and Integration Group.

The predictive analytical module in PHIS uses predictive models and algorithms to analyze real-time data.

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

PHIS does not use commercial (purchased or subscribed data feed from 3rd party sources) or publicly available data.

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

PHIS utilizes firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for IT. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act, subsection e[9], and OMB Circular A-108. All of the security controls in the system are reviewed annually or when significant modifications are made and re-authorization every three years. The SSP, and a subset of these controls, is also reviewed annually.

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

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

Controls are described in more detail in section 1.7 above.

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?

In accordance with Title 7 part 3015 Subpart D 3015.21: (a) Except as provided in paragraphs (b) and (c) of this section, records shall be kept for at least three years from the date specified in 3015:22. (b) If any litigation, claim, negotiation, audit or other action involving the records has been started before the end of the three year period, the records shall be kept until all issues are resolved, or until the end of the regular three year period, whichever is later. (c) In order to avoid dual recordkeeping; awarding agencies may make special arrangements for recipients to keep any records which are continuously needed for joint use. The awarding agency shall request a recipient to transfer records to its custody when the awarding agency decides that the records possess long-term retention value. When the records are transferred to or maintained by awarding agency the three year retention requirement shall not apply to the recipient.

All data retained from inspections will be considered accurate and relevant at the time the inspection was performed. Versioning will be used to track changes to the export library, inspection procedures and regulations. The furnishing of this information is voluntary and done by the record holder by filling out the required form.

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

Records will be destroyed or retired in accordance with USDA's published records disposition schedules, as approved by National Archives and Records Administration (NARA). A Master File backup is created at the end of the calendar year and maintained in accordance with General Records Schedule Authority N1-462-07-01, Item 2. System inputs are maintained in accordance with General Records Schedule Authority GRS 20, Item 2(a) (4), while system outputs (reports) are maintained in accordance with General Records Schedule Authority GRS 20, Item 16. PHIS does not currently destroy or retire any of its records.

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

The length of time data is retained does not change the level or type of risk associated with data retention. PHIS enforces encrypted, controlled access based on e-Authentication, timeout for remote access, and system audit logs to ensure information is handled in accordance with the above described uses. All authorized staff using the system must comply with the Agency's general use policy for IT. Rules of behavior

and consequences, and system use notifications are in accordance with the Privacy Act, subsection e[9], and OMB Circular A-130, Appendix III.

Section 4.0 Internal Sharing and Disclosure

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

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

PHIS shares information with the LIMS. Information is written to the database tables from the PHIS transactional database to be used by other systems including the Data Warehouse GSS. The FSIS data warehouse provides a source of legacy system data and analysis of inspection, audit, and assessment outcomes, and manages data from VetNet and PulseNet.

4.2 How is the information transmitted or disclosed?

PII data is not use for reporting or retrieval purposes.

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.

Privacy risks are minimized as the information collected (establishment name and address, along with personal names) is predominantly business related. Access to data is strictly controlled, access is granted through the USDA approved secure single sign on application (e-Auth – Level 2 Access) and authorization within PHIS is role based to ensure least privileges.

Section 5.0 External Sharing and Disclosure

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

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, all or a portion of the records or information contained in this system may be disclosed outside USDA as a routine use under 5 U.S.C. §552a(b)(3), as follows:

1. To the U.S. Department of Justice (DOJ)(including United States Attorney's Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary for the litigation and one of the following is a party to the litigation or has an interest in the litigation:

a. USDA or any component thereof;
b. Any employee of USDA in his/her official capacity;
c. Any employee of USDA in his/her individual capacity where DOJ or USDA has agreed to represent the employee; or
d. The United States or any agency thereof, and if the USDA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which USDA collected the records.

2. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the written request of the individual to whom the record pertains.

3. To the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

4. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function. This would include, but not be limited to, the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the Government Accountability Office, or USDA's Office of the Inspector General or any authorized representatives of that office.

5. To appropriate agencies, entities, and persons when:

a. USDA suspects or has confirmed that there has been a breach of the system of;

b. USDA has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and
c. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the

suspected or confirmed compromise and prevent, minimize, or remedy such harm.

6. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for USDA, when necessary to accomplish an agency function related to this system of records. Individuals who provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to USDA officers and employees.
7. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.
8. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or appropriate authority responsible for protecting public health, preventing or monitoring disease or illness outbreaks, or ensuring the safety of the food supply. This includes the Department of Health and Human Services and its agencies, including the Centers for Disease Control and Prevention and the Food and Drug Administration, other Federal agencies, and State, tribal, and local health departments.
9. To another federal agency or federal entity when USDA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the federal government or national security, resulting from a suspected or confirmed breach.

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.

Yes, the sharing of PII outside of the Department is compatible with the original collection and it is covered by an appropriate routine use in SORN, FSIS-2015-0015. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, all or a portionof the records or information contained in this system may be disclosed outside of USDA as a routine use under U.S.C. 552a(b)(3), as stated in the Notice and summarized here: To the Department of Justice for litigation purposes; to National Archives and Records Administration for records management; toa Congressional Office in response to an inquiry from therelevant constituent; to an

appropriate authority for audit purposes; to an appropriate authority in response to a threat or a confirmed breach to information security, programs and operations or confidentiality, when USDA has determined that there is a risk of harm to individuals, USDA, the Federal Government, or to national security and that disclosure is reasonably necessaryto assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm; to an appropriate law enforcement authorityin response to investigations, prosecutions, or enforcement actions; to contractors and agents performing a function on behalf of the Agency relating to the collection of information to support surveillance, investigations, and facilitation of rapid detection and response to foodborne hazards; to appropriate authorities, who are responsible for public health or monitoring illness outbreaks and ensuring the safety of the food supply, because the data supports officials in their ability to identify public health hazards and mitigate their impact through rapid communication and information sharingamong health and regulatory entities; to producing establishments in connection with the USDA/FSIS investigation of establishments and verification activities; to Other Users needing to verify electronic foreign health certificates for streamlining the import/export process; and to domestic and foreign publichealth entities seeking to prevent the cross-border movement of unsafe food supplies in advance of a shipment's arrival. All disclosures related to the domestic inspection, import/export and predictive analytic functions of PHIS are a routine use. The routine uses allow disclosures outside of USDA, which are either necessary for carrying out USDA's mission, or for minimizing waste, fraud, and abuse. In particular, such disclosures are required for USDA Personnel to carry out inspection and verification compliance activities and tomonitor the safety of products entering the country. On balance, the needs of USDA and the benefits to the other users, such as Other Government Officials and Business Personnel, justify the minimal impact on an individual's privacy.

.

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

Should PHIS 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.

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 is transmitted externally, there is the risk that it 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.

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.

USDA/FSIS-0004, Public Health Information System (PHIS)

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. Plant vendors are provided notification during business agreement processes.

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

Individuals do have the opportunity and/or right to decline to provide 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?

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

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

As notice is provided to inspection program personnel and contractors at the time of hiring, and to establishments when the plant applies for a grant of inspection, the risk associated with individuals being unaware of the collection is limited to establishment employees who may not have been made aware by their employer that a small subset of employee names may be contained in the system (in noncompliance reports, etc.). As inspection program personnel request names verbally on a regular basis, this risk is considered to be very limited.

Section 7.0 Access, Redress and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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

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

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

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?

The PHIS is accessed through the eAuthentication process. As individuals apply for eAuthentication credentials, they are provided access to the eAuthentication Privacy Act Statement which provides information on how their personal information will be protected. Additionally, FSIS provides a public facing PHIS Privacy Policy webpage containing privacy information and a contact for additional information.

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

Formal redress is provided.

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

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

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

To gain access to the PHIS, users must have a USDA e-Authentication user account and a role within the PHIS application. The requirement for the USDA e-Authentication user account is addressed in PHIS documentation along with the various PHIS roles.

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, authorized departmental contractors will have access to the system.

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

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

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

PHIS went through Security Assessment and Authorization and an ATO was granted on 03/23/2017 and will expire on 03/23/2020.

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

PHIS enforces encryption, controls access based on e-Authentication, forces a timeout after a specified period of inactivity, and maintains system audit logs.

Authorized user login identifiers are appended to system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system. Certain

PHIS tables have change data capture features turned on; this allows the database to retain old and new values along with who made the change and the time stamp.

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

Privacy risks are minimized as primarily business names and addresses, with limited individual names, are collected. All authorized users with access to 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-108. The security controls in the system are reviewed annually or when significant modifications are made to the system, re-authorization every three years

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?

PHIS is a major application.

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

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

Section 10.0 Third Party Websites/Applications

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

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

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

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

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

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

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

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

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

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

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

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

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

If so, is it done automatically?

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

If so, is it done on a recurring basis?

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

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

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

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

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

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

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

10.10 Does the system use web measurement and customization technology?

No.

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

N/A.

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

N/A.

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

N/A.

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

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

Responsible Officials

Carl A. Mayes
System Owner/Chief Information Officer
1400 Independence Ave SW
Washington, DC 20250

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

Privacy Office
1400 Independence Ave, SW
Washington, DC 20250

Approval Signatures

Barring any significant updates, signatures are not required until the ATO date of 03/17/2023.