



USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project.....	3
Mission Area System/Program Contacts.....	3
Abstract.....	4
Overview.....	4
Section 1: Authorities and Other Requirements	5
Section 2: Characterization of the Information	6
Section 3: Uses of the Information.....	10
Section 4: Notice	11
Section 5: Data Retention	12
Section 6: Information Sharing	13
Section 7: Redress	14
Section 8: Auditing and Accountability	15
Privacy Impact Assessment Review	16
Signature of Responsible Officials.....	16

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Web Services
Program Office	FSIS
Mission Area	Food Safety
CSAM Number	1751
Date Submitted for Review	10 April 2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Timothy Poe	timothy.poe@usda.gov	202-937-4207
Information System Security Manager	Rodney Sallie	rodney.sallie@usda.gov	202-708-9528
System/Program Managers	Shayla Bailey	shayla.bailey@usda.gov	202-690-6188

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

This document serves as the Privacy Impact Assessment for the Web Services System (WSS). The major function of WSS is to ensure the Internet site of FSIS at <https://www.fsis.usda.gov> and key partner web sites offer timely and accurate food safety and defense information.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The Food Safety and Inspection Service (FSIS) is the public health agency in the United States Department of Agriculture (USDA) that is responsible for ensuring that the nation's commercial supply of meat, poultry, and egg products is safe, wholesome, and correctly labeled and packaged.

The purpose of the WSS Team is to ensure that the Internet site of FSIS at www.fsis.usda.gov and key partner websites offer timely and accurate food safety and defense information. FSIS websites are an important tool in the communication of the agency's "public health through food safety and food defense" message. The key functions within the WSS Team are:

- Creating and managing content for the public internet site
- Reviewing and publishing content developed by other web authors/contributors
- Managing a limited amount of content on cross-agency portals
- Managing interactive tools, including the e-mail subscription service
- Monitoring Web metrics and key performance indicators

The FSIS WSS system is a Major Application (MA). It represents one of the components of FSIS communication to the American public and therefore, is essential to the FSIS mission of ensuring a safe and wholesome food supply for the Nation's population. WSS does not share personal information. However, it does provide information to the public.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

- 1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

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).

- 1.2. Has Authorization and Accreditation (A&A) been completed for the system?

Yes

- 1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

Not Applicable

- 1.4. Is the collection of information covered by the Paperwork Reduction Act?

Yes

Section 2: Characterization of the Information

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

- 2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

- | | | |
|---|--|--|
| ☐ Social Security number | ☐ Truncated or Partial Social Security number | ☐ Driver's License number |
| ☐ Passport number | ☐ License Plate number | ☐ Registration number |
| ☐ File/Case ID number | ☐ Student ID number | ☐ Federal Student Aid number |
| ☐ Employee Identification number | ☐ Alien Registration number | ☐ DOD ID number |
| ☐ Professional License number | ☐ Taxpayer Identification number | ☐ Business Taxpayer Identification number (sole proprietor) |
| ☐ Credit/Debit Card number | ☐ Business Credit Card number (sole proprietor) | ☐ Vehicle Identification number |
| ☐ Business Vehicle Identification number (sole proprietor) | ☐ Personal Bank Account number | ☐ Business Bank Account number (sole proprietor) |
| ☐ Personal Device Identifiers or Serial numbers | ☐ Business Device Identifiers or Serial numbers (sole proprietor) | ☐ Personal Mobile number |

☐ Health Plan Beneficiary number☐ Business Mobile number (sole proprietor)☐ DOD Benefits number**Biographical Information**☒ Name (Including Nicknames)☒ Business Mailing Address (sole proprietor)☐ Date of Birth (MM/DD/YY)☐ Ethnicity☐ Business Phone or Fax Number (sole proprietor)☐ Country of Birth☐ City or County of Birth☒ Group Organization/Membership☐ Religion/Religious Preference☐ Citizenship☐ Immigration Status☐ Home Phone or Fax Number☒ Home Address☐ ZIP Code☐ Marital Status☐ Spouse Information☐ Children Information☐ Military Service Information☐ Race☐ Nationality☐ Mother's Maiden Name☒ Personal Email Address☒ Business Email Address☐ Global Positioning System (GPS)/Location Data☐ Employment Information☐ Alias (Username/Scrennname)☐ Personal Financial Information (Including loan information)☐ Education Information☐ Resume or Curriculum Vitae☐ Business Financial Information (Including loan information)☐ Professional/Personal References**Biometrics**☐ Fingerprints☐ Hair Color☐ DNA Sample or Profile☐ Retina/Iris Scans☐ Video Recording

Distinguishing Features

- | | | |
|---|------------------------------------|-------------------------------------|
| ☐ Palm Prints | ☐ Eye Color | ☐ Signatures |
| ☐ Dental Profile | ☐ Photos | |

Characteristics

- | | | |
|--|--|---------------------------------|
| ☐ Vascular Scans | ☐ Height | ☐ Weight |
| ☐ Scars, Marks, Tattoos | ☐ Voice/Audio Recording | |

Device Information

- | | | |
|--|---|---|
| ☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones) | ☐ Cell Tower Records (e.g., Logs, User Location, Time) | ☐ Network Communication Data |
|--|---|---|

Medical /Emergency Information

- | | | |
|--|--|--|
| ☐ Medical/Health Information | ☐ Mental Health Information | ☐ Disability Information |
| ☐ Workers' Compensation Information | ☐ Patient ID Number | ☐ Emergency Contact Information |

Specific Information/File Types

- | | | |
|---|---|---|
| ☐ Personnel Files | ☐ Law Enforcement Information | ☐ Credit History Information |
| ☐ Health Information | ☐ Academic/Professional Background Information | ☐ Civil/Criminal History Information/Police Record |
| ☐ Case Files | ☐ Security Clearance/Background Check | ☐ Taxpayer Information/Tax Return Information |

2.2. What are the sources of the information in the system/program?

Members of the public

2.2.1. How is the information collected?

Information is entered manually by members of the public

- 2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No

- 2.4. How will the information be checked for accuracy? How often will it be checked?

Information can be checked and corrected by individuals at any time by submitting FOIA requests.

- 2.5. Does the system/program use third-party websites?

No

- 2.5.1. What is the purpose of the use of third-party websites?

Not Applicable

- 2.5.1.1. What PII will be made available to the agency through the use of third-party websites?

Not Applicable

- 2.6. **Privacy Impact Analysis:** Related to characterization of the information.

Follow the format below:

Privacy Risk: Web System Services (WSS) contains Personal Identifiable Information (PII) that can identify an individual, their residence, their email address (personal or business) and group or organizational affiliations. If PII is mischaracterized, it can inadvertently be supplied to unauthorized individuals.

Mitigation: WSS only collects the necessary PII for its intended business purposes. WSS clearly discloses its data collection practices and user rights along with adhering to relevant data privacy laws and standards are in accordance with the Privacy Act. The security controls in the system are reviewed when significant modifications are made to the system.

Section 3: Uses of the Information

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

- 3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Any PII provided will be used only for the intended purpose and maintained in accordance with the principles of the Privacy Act of 1974, the E-Government Act of 2002 and the Federal Records Act. Your information will not be disseminated to other entities.

- 3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

WSS does not use technology to conduct electronic searches, queries or analysis to identify a pattern or anomaly. WSS does not track web activities beyond the browsing of the website and does not cross-reference browsing activities with other entities.

- 3.3. **Privacy Impact Analysis:** Related to uses of the information.

Follow the format below:

Privacy Risk: WSS only uses the information collected for the intended purpose. WSS does not track or record information about individuals beyond browsing the website. Any information gathered from browsing activities is used to make the website more useful. Any PII provided by users of the website is not disseminated with other entities.

Mitigation: Any PII provided by users of the website is not disseminated with other entities. WSS utilizes firewalls and other security precautions such as role-based access and security hardening guides. All authorized staff maintaining 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 all applicable regulations and guidance.

Section 4: Notice

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

- 4.1. How does the project/program/system provide notice to individuals prior to collection?

Notice is provided on the webpage via the Privacy Policy link.

- 4.2. What options are available for individuals to consent, decline, or opt out of the project?

Individuals are not required to provide PII. PII is voluntarily provided by the individual.

- 4.3. **Privacy Impact Analysis:** Related to notice.

Follow the format below:

Privacy Risk: WSS website users may feel providing PII is required to interact with the website. Pressure felt to provide PII could result in individuals providing sensitive PII allowing for identity compromise. WSS website users may be unaware what data is being collected.

Mitigation: All PII is voluntarily provided by users interacting with the website. WSS does not collect any identifying numbers, biometrics information, medical/emergency information, device information, or specific information such as police records or credit history that would compromise someone's identity.

Section 5: Data Retention

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

5.1. What information is retained and for how long?

WSS retains information in accordance with USDA Departmental Regulation (DR) 3080-001, Records Management and FSIS Directive 2620.1 FSIS Records Management Program – Revision 5.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

WSS records are maintained in accordance with General Records Schedule (GRS) 6.5 Public Customer Service Records.

5.3. **Privacy Impact Analysis:** Related to retention of information.

Follow the format below:

Privacy Risk: Retention of information longer than necessary increases the chances of unauthorized exposure. Retaining information longer than necessary increases storage requirements, which increases storage costs.

Mitigation: WSS only retains information in accordance with GRS 6.5 Public Customer Service Records. WSS temporarily retains information for up to 1 year and is destroyed when no longer needed or deleted when superseded, obsolete or when a customer requests the agency to remove the records.

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

- 6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

WSS does not share information with other internal organizations.

- 6.2. **Privacy Impact Analysis:** Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: WSS does not share information internally with other entities. Information collected from WSS website users is only used to communicate with the user.

Mitigation: WSS only uses information collected for its intended business purposes. Information is not shared internally and retained per GRS 6.5.

- 6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

WSS does not share, receive or transmit information externally.

- 6.4. **Privacy Impact Analysis:** Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: Sharing information with external organizations increases the chances of unauthorized disclosure.

Mitigation: WSS does not share information external to the organization, thus, minimizing unauthorized access to minimal levels.

Section 7: Redress

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

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

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2168, 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: <https://efoia-pal.usda.gov>

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

Any individual who has reason to believe that WSS might have inaccurate or erroneous PII records pertaining to him or her should contact the FSIS FOIA Officer. The FOIA requestor must specify whether he or she wishes the records of the system to be checked.

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.

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

Redress is provided via the Privacy Policy.

7.5. **Privacy Impact Analysis:** Related to redress.

Follow the format below:

Privacy Risk: WSS website users may not be aware of how to ensure the accuracy of the information collected.

Mitigation: Before providing information, the individual is presented with a Privacy Act notice and an explanation of the Notice. The purpose, use, and authority for collection of information are described in the Privacy Act notice.

Section 8: Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

All USDA employees must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. USDA Contractors 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. All USDA users (employee or contractor) are required to take recurring security and privacy training that is conducted through the Office of the Chief Information Officer.

All authorized staff using a 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.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

The WSS website, www.fsis.usda.gov, is a forward-facing public website. Authentication isn't required for website users.

8.3. How does the program review and approve information sharing requirements?

WSS does not share information with other entities.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

All required training is taken online through AgLearn or through an external online training link for users who do not yet have network accounts. Security and privacy training is required during the onboarding process as well as on an annual basis.

Personally Identifiable Information (PII) Training provides in depth understanding of Personally Identifiable Information (PII). The course contains how to manage PII if lost, compromised or disclosed. In addition, it provides examples of non-PII, who is responsible for PII, identifies past PII incidents, PII policy, how to protect PII, how to encrypt documents, and how to report PII Incidents. Users have 90 days to complete the mandatory annual Information Security Awareness Training.

Privacy Impact Assessment Review

Approval Signatures:

Date reviewed by USDA Privacy Office: [4/25/2025](#)

Office of Chief Privacy Officer

United States Department of Agriculture

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Sign: _____

Shayla Bailey
System Owner
FSIS
U.S. Department of Agriculture

Sign: _____

Mission Area Privacy Officer
FSIS
U.S. Department of Agriculture

Sign: _____

Marvin Lykes
CISO/ACISO
FSIS
U.S. Department of Agriculture