Privacy Impact Assessment

Web Services System (WSS)

❖ Version: 1.4

❖ Date: February 3, 2022

❖ Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the Web Services System (WSS)

February 3, 2022

Contact Point

Shayla Bailey
Food Safety and Inspection Service
(202) 690-6188

Reviewing Official

Timothy Poe
FSIS Agency Privacy Officers
United States Department of Agriculture
(202) 205-3828

Abstract

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, the Intranet site at https://inside.fsis.usda.gov, and key partner Web sites offer timely and accurate food safety and defense information.

Overview

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, the Intranet site at http://inside.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 development and implementation of the Intranet site
- 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.

WSS is part of the Microsoft cloud fabric under the Azure Network General Support System (N-GSS) boundary which provides Internet service to the public and private (Intranet) service to FSIS employees. The public does not authenticate to any portion of WSS and only FSIS employees with a PIV card can access the FSIS Intranet. WSS is connected to the Internet to serve public Web pages; however, it is protected by USDA firewalls. WSS is not located in a harsh environment that would be detrimental to the hardware or to the system’s performance and availability.

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 website inside.fsis.usda.gov uses eAuthentication in the form of username and password.

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

WSS collects the information directly from the user of the system through the intranet site, https://inside.fsis.usda.gov.

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

The intranet site collects the information because it is required for users to access the site.

1.4 How is the information collected?

The information is collected when the user accesses the intranet site.

1.5 How will the information be checked for accuracy?

Access to the intranet site, https://inside.fsis.usda.gov is granted only to users with an FSIS employee eAuthentication account. The eAuthentication application is currently running version 2.0. FSIS users are granted access to different parts of the Intranet via Active Directory roles.

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.

WSS provides both public Internet service to the general public and private (Intranet) service to FSIS employees. Only FSIS employees with a PIV card can access the FSIS Intranet. WSS is connected to the Internet to serve public Web pages; however, it is protected by USDA firewalls. WSS is not located in a harsh environment that would be detrimental to the hardware or to the system's performance and availability. The public does not authenticate to any portion of WSS.

The public website provides links to several knowledge bases managed by FSIS personnel. Web managers within the FSIS Office of Public Affairs and Consumer Education (OPACE) perform system administration duties for the knowledge bases, but subject matter experts (SMEs) in the programs manage the content and work one-on-one with customers.

The Intranet application utilizes USDA's standard access control application to manage access to the Intranet; therefore, access is granted only to users with an FSIS employee eAuthentication account.

The eAuthentication application is currently running version 2.0. FSIS users are granted access to different parts of the Intranet via Active Directory roles. The Internet is open to all public users.

In summary, FSIS End Users use VPN and PIV cards through eAuth to access WSS. Access granted to end users, is approved by OPACE and they are given privileges based on a least privileged model.

Administrators Privilege users' access to WSS is restricted. Only three (3) persons have administrator access. Administrator access can only be achieved by VPN (if remote) and PIV Card access.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The FSIS intranet website inside.fsis.usda.gov uses eAuthentication in the form of username and password to get access to the FSIS intranet website. The information provided by the users will help ensure FSIS internal information is viewing by authorized user only.

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

The FSIS intranet website inside.fsis.usda.gov do not run any tool to analyze data.

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

WSS do not use commercial or publicly available data.

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

WSS utilizes 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 Office of Management and Budget (OMB) Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system.

USDA Enterprise Active Directory and FSIS intranet site's role-based security are used to identify the user as authorized for access and as having a restricted set of capabilities within the system. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer (OCIO), FSIS.

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

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 FSIS intranet website inside.fsis.usda.gov do not save the user's eAuthentication data after user login, the time is based on USDA eAuthentication session timeout for remote access.

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

N/A

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. WSS enforces encrypted, controlled access based on eAuthentication session timeout for remote access, and system audit logs to ensure information is handled in accordance with the above described uses. All authorized administrators 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?

The FSIS intranet website inside.fsis.usda.gov do not share the user's eAuthentication data after user login, it stored in the user browser session until the session timeout.

4.2 How is the information transmitted or disclosed?

WSS do not store the eAuthentication information, the eAuthentication session cookie expires after 30 minutes of inactive session, the information is not subjected to transmission or disclosure by WSS.

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.

Access to data is strictly controlled. Access is granted through Oracle database administrator privilege and authorization within an FSIS employee's role is based to ensure least privilege.

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?

Information is not shared with organizations external to the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

WSS does not share PII outside of the Department.

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

Should WSS 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.

N/A

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?

Yes, but without the eAuthentication login, the FSIS intranet access is denied.

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.

FSIS Privacy Policy is prominently displayed on the pages about the information collection process and usage.

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

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

WSS do not require you to provide PII to visit our website. Note, however, that you may be providing us with PII when you send us an e-mail message or a request for information or when you ask us to respond to a complaint.

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

The procedure is stated in FSIS Privacy Policy, which displays on every page of the WSS web sites: FSIS public site, FSIS intranet.

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

N/A – 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?

The Intranet application utilizes USDA's standard access control application to manage access to the Intranet; therefore, access is granted only to users with an FSIS employee eAuthentication account. The eAuthentication application is currently running version 2.0. FSIS users are granted access to different parts of the Intranet via Active Directory roles. The Internet is open to all public users.

8.2 Will Department contractors have access to the system?

Ordinarily no, however should a contractor be authorized to access the system; they will be governed by the contract's identifying Rules of Behavior (ROB) for USDA and FSIS systems and security. These types of contracts are routinely reviewed upon renewal by management and contract personnel expert in such matters.

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

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

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

Yes, this system was granted an ATO on 5/16/19.

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

WSS enforces encryption, controls access based on eAuthentication, forces a timeout after a specified period of inactivity, and maintains system audit logs.

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 with information limited to individual's first name, email address, eAuthentication username/password. All authorized staff using the system must comply with the Agency's general use policy for IT known as "Rules of Behavior and Consequences." System use notifications are in accordance with the Privacy Act, subsection e[9], and OMB Circular A-130, Appendix III.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

WSS is a major application.

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

No.

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.

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.

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

N/A.

10.12 <u>Privacy Impact Analysis</u>: 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

Shayla Bailey, FSIS-OPACE-DECS
United States Department of Agriculture

Approval Signature

Agreed: TIMOTHY POE (Affiliate) Digitally signed by TIMOTHY POE (Affiliate)
Date: 2022.05.04 14:58:11 -04'00'
Timothy Poe
Privacy Officer Date

Agreed: Shayla Mae Bailey Digitally signed by SHAYLA BAILEY
Date: 2022.05.04 15:04:46 -04'00'
Shayla Bailey Date
System Owner

Agreed: MARVIN LYKES Digitally signed by MARVIN LYKES Date: 2022.05.05 08:43:36 -04'00' ____________________

Marvin Lykes Date

Chief Information Security Officer (CISO)

Agreed: CARL MAYES Digitally signed by CARL MAYES Date: 2022.05.05 09:40:12 -04'00' ____________________

Carl A. Mayes Date

Assistant Chief Information Officer (ACIO)