

# Privacy Impact Assessment

USDA Meat and Poultry Hotline (Hotline)

- Version: 5.6
- Date: September 19, 2012
- Prepared for: FSIS





# **Privacy Impact Assessment for the USDA Meat and Poultry Hotline (Hotline)**

**September 19, 2012**



Document Revision and History			
Revision	Date	Author	Comments
5.3	September, 2011	James-P-Kurucz	Annual update
5.4	June, 2012	Ameya Thatte	New Template and few changes
5.5	August 2012	James Kurucz	Incorporated comments from the Privacy Office
5.6	September 19, 2012	James Kurucz	Incorporated CIO Comments

## **Abstract**

This document serves as the Privacy Impact Assessment for the USDA Meat and Poultry Hotline (Hotline). The purpose of the system is to provide information and collect feedback regarding the safety of meat, poultry, and egg products. This assessment is being done in lieu of the Privacy Threshold Analysis conducted in February 2011.

## **Overview**

The Food Safety and Inspection Service (FSIS) is obligated to protect safety of meat, poultry, and eggs, which are susceptible to the effects of naturally occurring phenomena, accidents, or intentional acts that affect the food supply chain. FSIS must detect threats and vulnerabilities as early and as specifically as possible so that it can mitigate them promptly.

The USDA Meat and Poultry Hotline is a toll-free telephone service that helps educate consumers to prevent foodborne illnesses, by answering their questions about safe storage, handling, and preparation of meat, poultry, and egg products. The Hotline also responds to other issues related to the mission of the FSIS, which helps to ensure that the Nation's commercial supply of meat, poultry, and egg products is safe, wholesome, and correctly labeled and packaged, as required by the Federal Meat Inspection Act, the Poultry Products Inspection Act, and the Egg Products Inspection Act.

As a centralized, one-stop call service for consumers from all 50 states, the District of Columbia, U.S. territories, and foreign countries, the Hotline is able to compare calls received from different regions of the country. In an emergency situation, such as an outbreak of foodborne illness, a natural disaster, or a product recall, the Hotline provides vital information in a timely manner. For example, in the event of a product recall, consumers can obtain detailed information that will help them identify the suspect product. Its nationwide service area also means that the Hotline can help detect possible public health threats. The Hotline is able to disseminate information widely through a variety of channels.

The USDA Meat and Poultry Hotline also serves as an "early warning" system. When consumers are concerned or confused about certain food safety issues, the Hotline is often the first to know. That feedback and information is critical to the development of the Agency's food safety education campaigns as well as its food safety policies. The Hotline is staffed by food safety specialists with backgrounds in home economics, nutrition, and food technology. The services provided by Hotline help to ensure that FSIS may continue to accomplish its mission of ensuring a safe and wholesome food supply for the Nation's population.

## **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?**

A person's name, address, and phone number is collected in two different instances. The first instance is collected when a caller to the Hotline wishes to file a complaint. This information is subsequently purged from the Hotline after the complaint is sent to Consumer Complaint Monitoring System II (CCMS II). The second instance is when a publication request is filed. The information resides in the Hotline until the Publication Manager releases the request.

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

Anybody who wishes to file a complaint or submit a publication request can be a source for information.

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

In the case of filing a complaint, the information is collected to uniquely identify the person on the complaint ticket sent to CCMS II. In the case of a publication request, the information is collected so that the publication can be shipped to the caller.

**1.4 How is the information collected?**

The information is collected via user agents who make inputs to the system.

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

The Hotline generates error messages to ensure appropriate data is entered into the proper fields. The administrator also runs monthly reports of all calls to the call center to ensure everything was entered appropriately.

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

US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate. USDA is also authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note) as well as TITLE 5 PART I CHAPTER 3 - 301, and 5 USC 552 - Sec. 552a

The Executive Order 9397 issued in 1943 allows Federal components to use the SSN exclusively whenever the component found it advisable to set up a new identification system for individuals, and requires the Social Security Board to cooperate with Federal uses of the number by issuing and verifying numbers for other Federal agencies.

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

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

The privacy risks are considered to be minimal because limited data is collected the data is readable by the publication manager in one case, and by the user agent in another case. Personally Identifiable Information (PII) cannot be used to retrieve data. Any privacy risk is estimated to be Low.

## **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.**

The data is used to initiate complaints and ship publications.

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

A system administrator can run reports on all of the calls to the center. No PII is kept in these reports. The reports are stored in a cabinet under lock and key.

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

No commercial or publicly available data is used in the system.

**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.**

Hotline limits the input of data by generating error messages when appropriate. It restricts date entry by using calendars when submitting date/time data. It uses dropdown menus where appropriate to limit information input. The system administrator runs reports on the calls monthly to check for accuracy. It is not possible to search for records using PII in the Hotline.

Furthermore, all call-specific data regarding complaints are electronically purged from the Hotline and forwarded to CCMSII when “enter” is hit. Call-specific data related to publication requests are purged as soon as the publication is mailed. More information on controls can be found in section 1.7.

## 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?

When a complaint is entered, the information will stay in queue until the user agent clicks the “Send to CCMS II: button. This usually lasts no longer than the call’s duration. Publication requests are purged when the publication requested is sent out.

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

Yes

### 3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data 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 retaining the data. Therefore, the same methods to reduce risk are used throughout the life of the data. The largest risk is that PII will be accessed by unauthorized users. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

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

In addition, logical access to the application and data is restricted to authorized personnel. 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.

Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

## **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?**

When a user files a complaint, the information is sent to the CCMS II staff for the purpose of generating a complaint ticket.

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

In the case of a complaint, Hotline transmits complaint data to CCMS II electronically once a call is finished. A publication request is stored in the database until a Publication Manager completes a batch.

### **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.**

The privacy risks are considered to be low because the information is only shared insofar as it is transferred between Hotline and CCMS II. PII Data are purged from Hotline upon transfer.

## **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?**

None

**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.**

N/A

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

N/A

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

N/A

## Section 6.0 Notice

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

**6.1 Was notice provided to the individual prior to collection of information?**

Notice is given to a caller at the beginning of a call.

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

It is made known to the caller that the complaint can be completed if the name and address are not given. If the caller declines, then the complaint will be submitted anonymously.

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

No.

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

Users are never unaware of data being collected. Notice is given to the users at the beginning of the transaction.

## **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?**

Users cannot access the data once submitted.

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

A new request is submitted to fix it.

For purposes of redress, individuals who have reason to believe that the Hotline might have records pertaining to them may also write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: [fsis.foia@usda.gov](mailto:fsis.foia@usda.gov).

The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country

and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

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

They would be advised if they called into the Hotline with questions about their information.

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

N/A.

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

There are limited privacy risks associated with redress. Redress will be handled primarily as specified above in Section 7.2.

## **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 Hotline 2.0 User Roles documentation clearly describes who has access to the system.

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

Yes, contractors support Operations and Maintenance of the system. Their use of the system is governed by contracts identifying rules of behavior for USDA and FSIS systems and security.

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

All users are required to undergo computer security training prior to accessing the system and must complete refresher training in order to retain access.

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

Yes.

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

The system is designed to limit incorrect data in the system and to limit access to data overall. The system also includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors. See section 1.7 for more information on controls.

**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?**

No serious privacy risks could be identified. It is also not possible to retrieve records using PII. The scope of the information collected is small. All of the Hotline staff has received training on the importance of safeguarding PII. Privacy risks are mitigated through annual training.

Overall, the privacy risk in this system is low. The Hotline has further mitigated this risks by granting access only to authorized personnel. Also, all USDA employees have undergone a background investigation and contractor access is governed by contracts identifying rules of behavior for USDA and FSIS systems and security.

## **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?**

Hotline 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”?**

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

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

N/A. Hotline does not use third-party websites

**10.10 Does the system use web measurement and customization technology?**

Hotline does not use web-measurement technology.

**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. Hotline does not use web-measurement technology.

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

N/A. Hotline does not use third-party websites



## Responsible Officials

Diane Van Lonkhuyzen  
System Owner  
5601 Sunnyside Ave. Room 2-L291 Mailstop 5269  
Beltsville, MD, 20705

Elamin Osman  
Chief Information Security Officer  
1400 Independence Ave SW Rm 4908  
Washington DC 20250

Janet Stevens  
Chief Information Officer  
1400 Independence Ave SW Rm 3165  
Washington DC 20250

Alicemary Leach  
Privacy Officer  
1400 Independence Ave SW Rm 1167  
Washington DC 20250

## PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: \_\_\_\_\_

**Diane Van Lonkhuyzen**  
Manager, USDA Meat and Poultry Hotline

\_\_\_\_\_

Date



## PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: <u><i>Diane Van Lonkhuyzen</i></u>	<u>8/29/2012</u>
<b>Diane Van Lonkhuyzen</b> Manager, USDA Meat and Poultry Hotline	Date
Agreed: <u><i>Elamin Osman</i></u>	<u>9/17/12</u>
<b>Elamin Osman</b> Chief Information Security Officer (CISO)	Date
Agreed: <u><i>Janet Stevens</i></u>	<u>9/25/12</u>
<b>Janet Stevens</b> Chief Information Officer	Date
Agreed: <u><i>Alicemary Leach</i></u>	<u>9-5-12</u>
<b>Alicemary Leach</b> Privacy Officer	Date