Privacy Impact Assessment

Consumer Complaint Management System II (CCMS II)

- Version: 2.5
- Date: September 28, 2012
- Prepared for: USDA OPHS HHSD

United States Department of Agriculture

Abstract

This document serves as the Privacy Impact Assessment for the CCMS II. The purpose of the system is to collect information, coordinate investigations and provide feedback regarding health risks associated with meat, poultry, and egg products, This assessment is being done in accordance with the Privacy Threshold Analysis conducted in February 2012.

Overview

The primary goal of CCMS II is to support and augment the Office of Public Health Science (OPHS) analysts in their ability to identify consumer health risks associated with FSIS regulated products. The system is designed to help analysts respond quickly and effectively to characterize possible threats to FSIS regulated products. FSIS developed the CCMS II database as a relational database for collecting sufficient information to assist FSIS with trace-back or trace-forward investigations to identify product disposition and/or the origin of hazards. This information also will be used to coordinate the recall of products when required.

At the completion of CCMS II development, CCMS 2.0 was installed on FSIS OCIO servers and User Acceptance Testing was successfully completed to ensure that the delivered system met the required functionality.

CCMS II is designed to be flexible and expandable for future integration with other Federal departments and agencies, other USDA agencies, state governments, and food safety and public health-related entities. CCMS II is being used by approximately 400-500 USDA users and the public via the World Wide Web.

For purposes of the CCMS II, a consumer complaint is any complaint meeting established criteria for handling by CCMS II as stated in FSIS Directive 5610.1, that is, a complaint regarding an FSIS regulated product reported to FSIS by a consumer or by someone on behalf of a consumer. This includes consumer complaints reported to FSIS by a state or local health department or a Federal agency, such as the Food and Drug Administration. It also includes complaints involving imported products that have been re-inspected by FSIS at the port of entry.

Consumer complaints are received through telephone calls to the USDA Field Compliance Officers and through the 1-800 number of the USDA Meat and Poultry Hotline. CCMS II also permits the public to enter complaint reports directly into Electronic Consumer Complaint System (ECCS). Adverse food event reports can also be received and managed for imported products and school lunch products distributed through USDA's Food and Nutrition Service. Complaints typically involve reports of illness, injury, foreign objects, contamination (including chemical contamination), allergic reactions, and improper labeling.

Processing Flow

a) CCMS II receives a complaint in one of the following ways: 1) a CCMS II analyst receives a complaint via phone and enters it into the system, 2) complaints are also

forwarded from the UDSA Meat and Poultry Hotline system, 3) Users are also able to submit complaint data into a web form that would then go through validation checking by a CCMS II analyst. Once approved the data will be entered into the CCMS II system.

b) If the complaint is received by a CCMS II User, the analyst logs on to the CCMS II application and enters all of the complaint information. If the complaint is forwarded from the USDA Meat and Poultry Hotline system; the CCMS II system sends an acknowledgement back to the USDA Meat and Poultry Hotline system.

c) Once the complaint has been entered, it is assigned to an analyst to review and perform any triage or research needed to determine the appropriate response.

d) All items related to the triage, research, investigation and advanced Agency actions related to an investigation are logged into the CCMS II system along with a resolution to the complaint.

e) If a case does not meet the criteria for handling by CCMS II as stated in FSIS Directive 5610.1 any additional actions needed to address the issue are taken outside the scope of CCMS II.

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 CCMS II system collects First Name, Last Name, Address, Phone Number, E-mail Address, and details of the complaint. Details of the complaint can include medical symptoms and medical treatment obtained, as well as information about the origin of the food item under consideration.

A unique case number is assigned to each case and provided to the individual who made the report. This reduces, but does not eliminate the need to retrieve information by personally identifiable information (PII).

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

Consumers or health care or public health professionals acting on behalf of a consumer are the originating source of information in the system. Information received from these individuals is manually entered into the system by a CCMS user or through a Web service that facilitates an import function from the Hotline database. Again, consumers can enter this information directly into ECCS.

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

The CCMS II collects the information to assist OPHS with trace-back or trace-forward investigations to identify product disposition and the origin of hazards related to consumer complaints associated with FSIS-regulated products.

1.4 How is the information collected?

Information will be collected directly by USDA/FSIS employees from consumers who have contacted a 1-800 number or a district office or by consumers who have accessed the web form. Information also may be collected from state and local departments of health or a Federal Agency, such as the FDA.

1.5 How will the information be checked for accuracy?

Data will be collected by trained analysts while speaking or interacting directly with the consumer or someone who is contacting FSIS on behalf of the consumer. These individuals bear the 'burden of proof' with respect to the accuracy and completeness. FSIS analysts, as part of any subsequent investigation, will confirm and correct, if needed, any inaccuracies.

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.

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

System Administrators and users of the system will have access. Authorized employees are assigned level-of-access roles based on their 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.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant

modifications are made to the system, but at least every three years. Active Directory and CCMS II 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. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.

By having a Department of Agriculture e-mail account, user network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. FSIS system users must pass a Government background check prior to having system access. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

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. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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 information provided will be used to identify, investigate, and respond to consumer health risks associated with FSIS-regulated product.

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

CCMS II has a query function that allows records contained within the database to be retrieved based on one or more data elements (e.g. complaint type, establishment number). An analytic component built into the CCMS II platform allows the user to compare complaints to other records in the system, so that related trends and clusters can be easily assessed. In addition, CCMS II features a GIS mapping capability that allows spatial data (such as complainant addresses) to be depicted on a map and analyzed for clusters.

Information recorded in CCMS that is converted into data fall into the following categories: complaint-specific (e.g. illness, foreign object), product-specific (e.g. canned, ready-to-eat, raw ground; product name, brand, lot numbers), plant-specific (establishment number), and point-of-purchase-specific (name and location).

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

CCMS II does not use commercially 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.

Access to CCMS II is restricted to trained, authorized employees, who require data that is accurate. Authorized employees are assigned level-of-access roles based on their 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.

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. CCMS II users enter their information into "cases" which are tracked and audited by the system and its administrators. Each case contains a case number, the date it was reported, the last activity performed on the case (by date), the establishment district, complainant district, the case's current status(draft**,** new, active, and closed) and managing organization. A user's actions on a case (created, modified, deleted) can also be tracked within the system.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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?

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA).

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

Yes, although discussions related to recent upgrades are being held.

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

There is no additional risk as a result of the length of time data is retained. However, as long as customer data is retained, there is the risk that it may be disclosed to unauthorized individuals. To mitigate this risk, the system is maintained in an access controlled facility and access controlled network. 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. 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.

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?

CCMS II pulls information from PBIS and Hotline in a one-directional connection and does not send any information back to PBIS. It does return a unique case number to the Hotline.

The Office of Field Operations and the Office of Program Evaluation, Enforcement and Review have direct access to the CCMS II System. Both offices input complaints and are assigned tasks via CCMS II for investigations and other complaint follow-up activities.

4.2 How is the information transmitted or disclosed?

N/A

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.

See Section 1.7 above. To minimize any risks, all FSIS systems are continuously monitored by Security Operation Center (SOC) and by the Infrastructure Operations Division (IOD) Engineering Branch to ensure that FSIS data is handled in accordance with the FSIS security policies.

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?

Routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

In some cases, a consumer complaint will need to be forwarded to an agency outside of FSIS (e.g., state and local department of health and Food and Drug Administration) for follow-up or review, or because the product is outside FSIS' jurisdiction. In such cases, a printed record of the complaint is forwarded via email or fax by the CCMS II analyst to a point-of-contact at the appropriate agency. As a safeguard, notification is sent beforehand to this point-of-contact to alert them of the incoming information, to help ensure the protection of potentially sensitive information.

In addition, information related to an outbreak is sometimes shared with the Centers for Disease Control and Prevention. This information is not related to an individual and does not contain any PII.

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.

Under normal circumstances, CCMS II does not share PII outside the department. However, routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

In some cases, a consumer complaint will need to be forwarded to an agency outside of FSIS (e.g., state and local department of health and FDA) for follow-up or review. In such cases, a printed record of the complaint is forwarded via email or fax by the CCMS II analyst to a point-of-contact at the appropriate agency. As a safeguard, notification is sent beforehand to this point-of-contact to alert them of the incoming information, to help ensure the protection of potentially sensitive information. FSIS Directive 5610.1 states that complaints concerning products that are not under FSIS jurisdiction (e.g. retail-prepared foods) should be reported to the proper authority (e.g. state/local health departments).

A SORN has been created for this system.

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

In some cases, a consumer complaint will need to be forwarded to an agency outside of FSIS for follow-up or review. In such cases, a printed record of the complaint is forwarded via email or fax by the CCMS II analyst to a point-of-contact at the appropriate agency. As a safeguard, notification is sent beforehand to this point-of-contact to alert them of the incoming information, to help ensure the protection of potentially sensitive information

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

Risks include the release of PII to persons/entities for whom it was not intended.

Mitigation includes giving prior notification to persons/entities prior to record sharing and restricting the level of record-sharing to person/entities on a need-to-know basis.

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?

Yes. This notice is provided verbally by Hotline staff and via ECCS to consumers entering complaints.

The ECCS notice provides information about FSIS' privacy policy, and identifies that information may be shared with other agencies if the product is not under our jurisdiction or if there is any investigation required.

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

Yes.

Information is given voluntarily to FSIS. Individuals retain the right to report a complaint anonymously and can decide not to provide information.

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.

Data will be collected by trained FSIS analysts while speaking or interacting directly with the consumer. The customer will be provided notice to the particular uses of the information at the time they call to register their complaint. Individuals retain the right to report a complaint anonymously and can decide not to provide information, but they do not have the option to determine how we use the information that *is* provided for investigative purposes.

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?

At the time of contact, callers are provided a unique case number. They can use that case number to follow-up with FSIS to obtain information regarding the status of any investigation resulting from their call.

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

As noted in Section 7.1, should callers wish to correct information on a pending investigation, they can follow-up using the unique case number they were provided.

In addition, individuals who have reason to believe that this system might have records pertaining to them should 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. Personnel in that division will then forward the request to the USDA agency that they believe is most likely to maintain the records the individual is seeking.

The individual must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; current mailing address and zip code; signature; CCMS II case number, if applicable and known; and 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.

For more information about how to make a FOIA request, please see http://www.fsis.usda.gov/FOIA/FOIA_Request/index.asp.

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

When the caller is provided with the case number, they are advised that they can follow-up.

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

N/A- See Section 7.2

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 additional 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?

System Administrators and users of the system will have access. Authorized employees are assigned level-of-access roles based on their 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.

To gain access to the CCMS II system, a user must have 1) an account on the FSIS Active Directory; 2) a job function in an FSIS office requiring access to CCMS II according to FSIS Directive 5610.1; and 3) an assigned role within the CCMS II application. CCMS II access procedures are also defined in the CCMS II SOP.

8.2 Will Department contractors have access to the system?

Yes.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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

Prior to system access, all users are required to undergo Department-approved computer security awareness training that includes a privacy component and must complete computer security training yearly in order to retain access.

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

Yes, the ATO was granted on 11-Aug-2010.

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

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

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. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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

The primary risks are that the customer information may be incorrect or that it may be disclosed to unauthorized individuals. These risks are mitigated by the following safeguards.

System Administrators and users of the system will have access. Authorized employees are assigned level-of-access roles based on their 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.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every 3 years. Active Directory and CCMS II 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. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.

By having a Department of Agriculture e-mail account, their network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. FSIS system users must pass a Government

background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

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. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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?

CCMS II 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 - Third party websites are not being used.

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?

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

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

Regina Tan – Director, Epidemiology Division
Office of Public Health Science
United States Department of Agriculture

Alicemary Leach – Director, ECIMS
Office of Public Affairs and Consumer Education
United States Department of Agriculture

Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

Janet Stevens – Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

Approval Signatures

Regina Tan
Director, Epidemiology Division
Office of Public Health Science
Food Safety and Inspection Service
United States Department of Agriculture

Alicemary Leach
Director ECIMS
Office of Public Affairs and Consumer Education
Food Safety and Inspection Service
U.S. Department of Agriculture

for Elamin Osman
Chief Information Security Officer
Food Safety and Inspection Service
Office of the Administrator
United States Department of Agriculture

Janet Stevens
Chief Information Officer
Food Safety and Inspection Service
Office of the Administrator
United States Department of Agriculture