# U.S. DEPARTMENT OF AGRICULTURE

## PRIVACY IMPACT ASSESSMENT

VERSION 1.4

**OFFICE OF THE CHIEF PRIVACY OFFICER**

# Privacy Impact Assessment

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

*The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).*

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

**Guidance on how to complete the following PIA Questionnaire is available** here.

# Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:

***Research Conducted by Third Party Contractors for the***

***Office of Public Affairs and Consumer Education***

***Food Safety Inspection Service***

Date PIA submitted for review:

***January 29, 2024***

Mission Area System/Program Contacts:

| | **Name** | **E-mail** | **Phone Number** |
|---|---|---|---|
| Mission Area Privacy Officer | Timothy Poe | Timothy.poel@usda.gov | 202-937-4207 |
| Information System Security Manager | Mesay Amberber **Director of IT Operations** | mamberber@forsmarsh.com | 571-444-1136 |
| System/Program Managers | Jeremy Vanderlan **CTO** | jvanderlan@forsmarsh.com | 571-384-4066 |

**Abstract**

The United States Department of Agriculture, (USDA) Food Safety Inspections Service (FSIS) uses contractor third parties and their subcontractors to conduct market research. The contractors use the Microsoft SharePoint application to store data collected from the research efforts. Microsoft SharePoint is owned by the contractors, and personally identifiable information (PII) such as names, telephone numbers, and email addresses are collected from recruited research project participants as part of the efforts on projects. The PII is held by the contractor and no PII data is delivered to the FSIS.

**Overview**

The U.S. Department of Agriculture (USDA), Food Safety Inspection Service (FSIS), Office of Public Affairs and Consumer Education (OPACE) ensures that members of the American public are equipped with the tools they need to reduce their risk of foodborne illness by teaching others how to safely handle, prepare, and store food. OPACE staff are responsible for designing and implementing education efforts to promote safe food handling procedures and reduce the likelihood of foodborne illness.

In some education efforts OPACE contracts with third party service providers to recruit, identify, and interview members of the public, and provide research information for the agency. The contractors may also employ subcontractors in the process. Contactor and subcontractor efforts may include the collection of Personally Identifiable Information (PII) and sensitive data.[1]

Contractors may use system applications such as Microsoft SharePoint to store collected data from the research projects. The applications are owned by the contractors, and the stored data may include PII such as names, telephone numbers, email addresses, ethnicity, and gender. The applications are also used to facilitate communication with interview participants (typically through email).

Research project participant interview responses are not shared with the public. Within the application, information is stored in password protected folders, and a limited number of contractor personnel (Project Directors, Project Managers, and Senior Analysts), and subcontractor personnel have access to the PII.

No PII will be shared by the contractors or subcontractors with FSIS. The data in the contractor's control will be held no longer than 120 days from contract end, and the PII will be deleted from the application and any other backup systems.

# Section 1.0 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] For example, whether someone has a living parent or in-law who is 65 years of age or older, and what language is spoken at home,

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

Generally speaking, the authorities for USDA to collect, maintain, use and disseminate information 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).

Regarding the authorities that allow the USDA to collect information in research endeavors described herein this document, the 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?

No Authorization and Accreditation has been completed for this system by FSIS. SharePoint is owned by the contractor and the contractor is responsible for maintaining appropriate authorization and accreditation of the system

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

No current Food Safety Inspection Service System of Records Notices apply to the information collected. Although the contractor is collecting PII as part of its research tasks, the PII data is not used to search the SharePoint system. Additionally, no PII data is delivered to FSIS.

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

This information collection is covered by the Paperwork Reduction Act through OMB FSIS 2023-0011-0001. The collection instruments are provided in an appendix to this document.

# Section 2.0 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?

# Privacy Impact Assessment

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 | | | ☐ | License Plate Number |
| ☐ | Registration Number | | | ☐ | File/Case ID Number |
| ☐ | Student ID Number | | | ☐ | Federal Student Aid Number |
| ☐ | Passport number | | | ☐ | Alien Registration Number |
| ☐ | DOD ID Number | | | ☐ | DOD Benefits Number |
| ☐ | Employee Identification 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 | | | ☐ | Business Mobile Number (sole proprietor) |
| ☐ | Health Plan Beneficiary Number | | | | |
| **Biographical Information** | | | | | |
| ☒ | Name (including nicknames) | ☒ | Gender | ☐ | 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 |
| ☐ | Citizenship | ☐ | Immigration Status | ☐ | Religion/Religious Preference |
| ☐ | Home Address | ☐ | Zip Code | ☐ | Home Phone or Fax Number |
| ☐ | Spouse Information | ☐ | Sexual Orientation | ☐ | Children Information |
| ☐ | Marital Status | ☐ | Military Service Information | ☐ | Mother's Maiden Name |
| ☒ | Race | ☐ | Nationality | ☐ | Global Positioning System (GPS)/Location Data |
| ☒ | Personal e-mail address | ☐ | Business e-mail address | ☐ | Personal Financial Information (including loan information) |
| ☐ | Employment Information | ☒ | Alias (username/screenname) | ☐ | Business Financial Information (including loan information) |
| ☐ | Education Information | ☐ | Resume or curriculum vitae | ☐ | Professional/personal references |

| Biometrics/Distinguishing Features/Characteristics | | | | | |
|---|---|---|---|---|---|
| ☐ | Fingerprints | ☐ | Palm prints | ☐ | Vascular scans |
| ☐ | Retina/Iris Scans | ☐ | Dental Profile | ☐ | Scars, marks, tattoos |
| ☐ | Hair Color | ☐ | Eye Color | ☐ | Height |
| ☐ | Video recording | ☐ | Photos | ☒ | Voice/ Audio Recording |
| ☐ | DNA Sample or Profile | ☐ | Signatures | ☐ | Weight |
| **Medical/Emergency Information** | | | | | |
| ☐ | Medical/Health Information | ☐ | Mental Health Information | ☐ | Disability Information |
| ☐ | Workers' Compensation Information | ☐ | Patient ID Number | ☐ | Emergency Contact Information |
| **Device Information** | | | | | |
| ☐ | Device settings or preferences (e.g., security level, sharing options, ringtones) | ☐ | Cell tower records (e.g., logs, user location, time, etc.) | ☐ | Network communications data |
| **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 |

Additional information collected may include (a) whether someone has a living parent or in-law who is 65 years of age or older and (b) what language is spoken at home, (c) whether participants have children living at home (NOTE – no other information will be requested regarding children).

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

The information is collected directly from individuals by a commercial recruitment firm and contractor staff, who will conduct the interviews. Information is collected to identify individuals who would be eligible to participate in an interview among the focal population related to food safety behaviors, and to gather information that will answer the research questions. Information will not be collected from sources other than directly from the individual.

### 2.2.1. How is the information collected?

The information will be collected directly from the individual through phone call screening and video web conferencing interviews.

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

Research projects will not collect information through any commercial sources or publicly available data.

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

During the phone screening, screeners restate responses to individuals to affirm the accuracy of the information collected. If a participant wishes to review his/her screening and interview responses, the project team will email interview notes to the participant, who can then note changes.

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

Yes

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

A third-party application such as Microsoft SharePoint is used to store basic biographical information gathered during recruitment, such as participant names, gender, race, ethnicity, country of birth, and children living at home. The application is also used to facilitate communication with interview participants (through email) and to communicate with them about the day and time of their interview.

### 2.5.1.1. What PII will be made available to the agency though the use of third-party websites or applications?

No personal identifiable information will be made available to the Agency through the use of third-party websites or applications.

### 2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

**Privacy Risk**:

The purpose of the information collected is to allow contractors to identify participants in food safety research projects.

Potential risk is possible in gathering the wrong information, or more than the minimum amount of information needed will be collected in the research projects.

**Mitigation**:

Information collected will be directly relevant to the purpose of this project. No highly sensitive information, such as social security numbers, or health status information (e.g., history of food-borne illness) will be collected. Interview participants will also be clearly informed of what information will be collected, how their information will be used, and their freedom to decline participation in the project.

All information will be collected in a timely manner and will be deleted within 120 days of data collection completion.

# Section 3.0 Uses of the Information

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

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

Personal information is collected for the sole purpose of improving the effectiveness of consumer education messaging. Collecting personal information is also necessary to ensure that individuals providing feedback on the educational messages are also members of the audiences of focus for projects.

### 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.

The projects will not use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate predictive patterns or anomalies.

### 3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

**Privacy Risk**:

Personally identifiable information collected from participants may be used for purposes outside the parameters of contracted research projects.

**Mitigation**:

The data and information are secured. A limited number of contractor personnel have access to the research project participant interview responses, which will not be shared with the public. Within the application, information will be stored in a password protected folders, and a limited number of contractor personnel (Project Directors, Project Managers, and Senior Analysts) and subcontractor personnel have access to the PII.

The information collected will be directly relevant to the purpose of this project. No highly sensitive information such as social security numbers, or health status information (e.g., history of food-borne illness) will be collected. All information will be collected in a timely manner and will be deleted within 120 days of data collection completion.

# Section 4.0 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 about the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information will be provided to potential interview participants through a plain-language informed consent document. This information will also be read allowed to participants before consent is requested.

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

All individuals will be provided with a description of their rights as a participant (in verbal and written format) and will be given the option to decline or opt out of the project. No individuals will participate in the project unless their explicit and verbal participation is provided.

### 4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

**Privacy Risk**:

Information is collected to identify individuals eligible to participate in an interview among the focal population related to food safety behaviors, and to gather information that will answer food safety research questions. The privacy risk is participants might take part in projects without full notice that PII will be gathered as part of the process.

**Mitigation**:

Interview participants are clearly informed of what information will be collected, how their information will be used, and their freedom to decline participation in the project. All information will be collected in a timely manner and will be deleted within 120 days of data collection completion. The notice provided to potential participants corresponds to the need to fully inform participants in market research projects gathering data and information.

# Section 5.0 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?

Data will be retained by the contractor for within 120 days after the interviews are completed. The 120-day period will be used to ensure that the data can be revisited if any questions arise relating to the project or the demographic characteristics of the participants. All data will be removed from the application and destroyed 120 days after the final interview date.

### 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.

No records will be held by the Food Safety Inspection Service. The data and information will be held by the contractor.

**5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.**

**Privacy Risk**:

Not applicable

**Mitigation**:

Not applicable

# Section 6.0 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?**

The non-aggregated PII will not be shared directly with any USDA or federal program offices or IT system within the USDA. The information will only be shared and stored on the contractor's application in a password protected folder.

**6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.**

**Privacy Risk**:

Not applicable

**Mitigation**:

Not applicable

**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?**

The information will only be shared between subcontractors (recruitment vendors) and contractors (the project contractor). Information will be transmitted through an encrypted folder and later stored in a password protected folder on the application When transmitting this data, encryption will be used to enhance security of the transmission process. This information will not be shared with any other entities outside of the organizations stated.

**6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.**

**Privacy Risk**:

Information sharing could result in privacy incidents and breaches if not properly handled.

**Mitigation**:

Information will not be shared within the USDA. All information will be stored in a password protected folder on the application, and encryption used when sharing occurs between the contractors and subcontractors.

# Section 7.0 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?

If a participant wishes to review his/her screening and interview responses, the project team will email screening responses and interview notes to the participant.

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

If a participant requests changes to the screening or interview responses, the project team will make those changes. The email with the participant's screening and/or interview responses will provide a Senior Analyst's name and email address to contact if the participant wishes to correct inaccurate or erroneous information.

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

At the end of the interview, the project team member conducting the interview will verbally notify the participant of the process for formal redress. The project team member will state, "After this interview, you have an opportunity to correct your information. You may ask for a copy of any answers you gave during an earlier call to see if you qualified for today's interview. You may also ask for a copy of any answers you gave during today's interview. To make the request, email [Senior Analyst] at [email address].You will get a response with your answers within 5 business days."

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

Formal redress is provided.

### 7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

**Privacy Risk**:

The privacy risk is failure in the redress process and individuals being unaware of how to correct inaccurate information.

**Mitigation**:

Project team interviewer will verbally notify the participant of the process for formal redress as described above stating, “After this interview, you may ask for a copy of any answers you gave during an earlier call to see if you qualified for today’s interview. You also may ask for a copy of any answers you gave during today’s interview. To make the request, email [Name of Senior Analyst] at [Analyst’s email address]. You will get a response with your answers within 5 business days.”

# 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?

PII collected on projects by contractors will be securely stored in a password protected folder on Microsoft SharePoint. Project team members must complete the privacy training detailed in 8.4 before getting the password. If personnel no longer require access to the information, the password will be changed and remaining project team members will receive the new password. Encryption and timely destruction of information will be used to enhance security.

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

Encryption is used to protect data in transit, and a password protected folder is used to protect data at rest. The data is also encrypted at rest within the database. A limited number of personnel employed by the contractor will have access to this password protected folder to ensure personal information is only accessed by those who require it for analysis and reporting purposes.

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

All sharing requirements are reviewed by the Director of Food Safety Education Staff, FSIS. If any access requirements change, the Director will be notified, and approval of the change will be requested.

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

All project team members will have Collaborative Institutional Training Initiative (CITI) certificates. In addition, the Fors Marsh Project Director will conduct a training that will provide an overview of data protection laws and regulations, human subjects protection and informed consent procedures, data collection procedures, sensitivity training, data analysis and reporting, and data management and security steps; and involve a discussion to prepare the SAGO recruiter and the Fors Marsh Project Manager and Senior Analyst for any challenging situations they might encounter during participant recruitment and data collection.

Additionally, all team members will complete the USDA Security Awareness and Rules of Behavior training.

Approval Signatures:

_____
Timothy Poe
Mission Area Privacy Officer
Food Safety Inspection Services
United States Department of Agriculture

_____
CISO/ACISO
Food Safety Inspection Services
United States Department of Agriculture

_____
David Lindner
Chief Privacy Officer
United States Department of Agriculture