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 for the USDA IT System/Project:

Hearing Conservation Program

Office of Management (OM)

Safety and Physical Security Branch

Date PIA submitted for review:

Thursday, February 15, 2024

Mission Area System/Program Contacts:

	Name	**E-mail**	
Mission Area Privacy Officer	Timothy Poe	Timothy.Poe@usda.gov	202-937-4207
Information System Security Manager	Marvin Lykes	Marvin.Lykes@usda.gov	202-515-6115
System/Program Managers	Tauseef Badar	Tauseef.Badar@usda.gov	202-440-3901

Abstract

Due to increased variability of working conditions and noise exposure levels at worksites, the Food Safety Inspection Services (FSIS) implemented the Occupational Safety and Health Administration's general requirement to establish a Hearing Conservation Program (HCP). The program requires annual audiogram testing of personnel to ensure we meet the requirements of the HCP. A contractor will be engaged to provide program services in accordance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) regulations. A Privacy Impact Assessment is required because the program gathers personally identifiable information.

Overview

The Food Safety Inspection Services (FSIS) on-site personnel work near tools, equipment, and machinery at food processing and slaughter plants that potentially exposes them to damaging noise levels. Due to the noise exposure levels within the plants, the USDA implemented the Occupational Safety and Health Administration's (OSHA) general requirement to establish a Hearing Conservation Program (HCP).

FSIS personnel working in locations with potentially hazardous noise levels have the option to enroll in the HCP.[1] Participants may undergo one annual self-administered audiometric exam using a Portable Audiometric Testing Device. The test will be reviewed by a professionally trained and certified audiologist to evaluate the participant's hearing. FSIS currently conducts these examinations on an ad hoc basis through verified vendors across USDA's multiple Districts.

FSIS will engage a contractor to administer the HCP, and as part of the effort the contractor will have an electronic record-keeping database that stores all audiogram tables, or audiometric test charts, as specified in 29 CFR 1910.95(m)(1).[2] For each employee tested, the database will provide a historical record that includes the employee's name, date of birth, job classification, date and time of test, audiologist's name, evaluation comment, hearing thresholds, and a brief indication of any significant problems noted by employee at time of test.

FSIS will establish a secure server that adheres to robust encryption protocols and incorporates identity and access management controls through multifactor identification. This server will facilitate the secure exchange of data between the vendor supporting HCP for FSIS employees, and the FSIS HR staff who require access.

[1] The employer shall establish and maintain an audiometric testing program as provided in this paragraph by making audiometric testing available to all employees whose exposures equal or exceed an 8-hour time-weighted average of 85 decibels. See 29 CFR 1910.95(g)(1).
[2] The employer shall maintain an accurate record of all employee exposure measurements required by paragraph (d) of this section. See 29 CFR 1910.95(m)(1).

The Office of the Chief Information Officer (OCIO)-created secure server will be able to access audiograms by District Office/establishment location or by individual name, and test results will be populated immediately after completed testing. The information collected and maintained by the contractor will be subject to the privacy standards in the Health Insurance Portability and Accountability Act (HIPAA).[3] FSIS will additionally require contractors to sign a Non-Disclosure Agreement.

The contractor will also provide tabular or charted summaries of the audiometric test data to each District Office and to Administrative Services Division Safety & Physical Security Branch Industrial Hygienist for review within 30 days of the original audiometric test date. All employee audiograms and records must be handled in accordance with Privacy Act requirements.[4]

For each test performed, a summary report will provide written notification of the test results for each employee tested. The notification is a written description of the status of the employee's threshold sensitivity as measured on the most recent audiometric test to that of the most recent baseline.

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.

1.1. 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 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

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[4] 1910.95(m)(4) Access to records. All records required by this section shall be provided upon request to employees, former employees, representatives designated by the individual employee, and the Assistant Secretary.

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).

Specifically related to the Hearing Conservation Program, the Occupational Safety and Health Administration (OSHA), promulgated OSHA 29 CFR 1910.95, regarding noise exposure, and testing. USDA/FSIS is administering the hearing test program for personnel exposed to high sound levels in their work environment.[5]

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

The data related to the HCP will be stored on a secure server in the HR-GSS IT System boundary which is a moderate level system that has a current Authority to Operate (ATO) in the FSIS production environment. Security assessment activity is done annually to ensure FISMA compliance with applicable controls to safeguard tenets of confidentiality, integrity, and availability.

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

SORN OPM/GOVT–10 applies to the information.

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

No. Data collected is solely on FSIS employees and not the public.

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?

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.

[5] The USDA HCP administers to personnel whose work environments generate noise exposure levels greater than or equal to an 8-hour time-weighted average (TWA) sound level of 85 decibels. All FSIS In-Plant Personnel (IPP) have the option to enroll in the HCP given their ubiquitous exposure to hazardous noise levels unless noise dosimetry monitoring confirms otherwise.

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 includes the employee's job classification, date and time of the hearing test, the test examiner's name, an evaluation comment, hearing thresholds, and a brief indication of any significant problems noted by employee at time of test.

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

Program participants are the source of the information.

2.2.1. How is the information collected?

Information is collected from participating FSIS personnel during the testing process using Portable Audiometric Testing Devices. The device may be an iPad, tablet or other mobile device running the vendor's testing software.

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

No

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

Th portable devices require annual calibration per OSHA guidance. Additionally, during testing the device will stop if the noise level in the environment exceeds 40 decibils thereby ensuring the test is accurate.

Participants will be responsible for checking their personal information and contacting FSIS Human Resources to update records.[6]

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

No

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

Not applicable.

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

Not applicable.

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

Privacy Risk: Unintended disclosure of the collected health information.

Mitigation: The collected information is safeguarded by leveraging the Transport Layer Security 2.X (TLS 2.X) encryption across the communication medium between the vendor and location point where the data resides. The disk storage area is encrypted for data at rest, which protects confidentiality. Additionally, an in-line web application firewall proxy service is in place restricting malicious activity (i.e. Distributed Denial of Service attacks, BOT attacks, and Orchestration attacks).

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?

[6] Voluntary participation in the program is annual.

Due to increased variability of working conditions and noise exposure levels within processing and slaughter plants, the information collected in the HCP helps to prevent initial occupational hearing loss by equipping personnel with the knowledge and hearing protection devices necessary to safeguard themselves.

The PII collected as part of the program allows staff to monitor work conditions and personnel health and safety.

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.

Yes. The program will use analysis of results to determine if there is an issue in a particular facility.

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

Privacy Risk: There is a risk that the hearing test information may be used in a way other than its intended purpose. For example, an unintended use could be marketing or advertisements to the program participants.

Mitigation: To mitigate this risk, the vendor will sign a Non-Disclosure Agreement outlining the data collected and its appropriate uses.

Note: the information will be secured by leveraging the Transport Layer Security 2.X (TLS 2.X) encryption across the communication medium between the vendor and location point where the data resides. The disk storage area is encrypted for data at rest, which protects confidentiality. Additionally, an in-line web application firewall proxy service is in place restricting malicious activity (i.e. Distributed Denial of Service attacks, BOT attacks, and Orchestration attacks).

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?

FSIS personnel who agree to register and participate in the HCP Program will generally follow the OPM/GOVT–10 SORN information regarding consent and uses of the information collected.

The Portable Audiometric Testing Device will contain an electronic Privacy Act Statement page describing the authority, purpose, and uses of the collected information as well as a link to the related SORN.

Regarding collection of health-related information, notice is additionally given to affected FSIS personnel via Form 4339-1during the on-boarding process. The principal purpose of the form is to obtain medical information from FSIS current and prospective employees to assist in determining medical fitness for duty.[7]

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

Personnel are not required to participate in the program. If an FSIS employee chooses to not participate then that person will be asked to sign a "Declination Statement." The declination statement is maintained in the employee's Medical File by HR.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: Individuals may not understand participation is voluntary and how to opt out of participation.

Mitigation: Participation in the testing program is voluntary, and the Portable Audiometric Testing Device will contain an electronic Privacy Act Statement page describing the authority, purpose, and uses of the collected information as well as a link to the related SORN.

Participants can also obtain additional program information by contacting FSIS Human Resources: 1-877-374-7471 to reach FSIS HR representatives Monday-Friday from 8:00 a.m. to 4:00 p.m. Participants may also mail FSISH1@usda.gov.

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?

Testing information and related PII (noted above) collected from the participants in the HCP is retained by FSIS per the standards in the OSHA regulatory requirements. Information collected will be retained by FSIS for the entire period of the employees federal/civilian service per OSHA CFR 1910.95.[8]

[7] Additional potential uses of the information include using it to ensure fair and consistent treatment of employees and job applicants and to adjudicate claims of discrimination under the Rehabilitation Act of 1973, as amended. This form is only used to collect medical information about applicants during the post-offer phase of hiring or to collect medical information about employees when job-related and consistent with business necessity.

[8] 1910.95(m)(3) Record retention. The employer shall retain records required in this paragraph (m) for at least the following periods.1910.95(m)(3)(i) Noise exposure measurement records shall be retained for two years. 1910.95(m)(3)(ii) Audiometric test records shall be retained for the duration of the affected employee's employment.

The HCP contractors are subject to HIPAA guidelines and standards regarding documents and retention. Contractor will hold records for six years and then dispose of them.

We note that since 1984 the Employee Medical Folder has been used to store long-term occupational medical records that were created during an employee's Federal career. These records do not include records on claims filed under the Federal Employee's Compensation Act. When an employee for whom there are long-term occupational medical records separates from Federal service, the last employing agency sends the Employee Medical Folder to the National Personnel Records Center. The National Personnel Records Center retains these Folders for 30 years after separation.

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.

The retention schedule for the HIPAA data collected is approved by the USDA records office and NARA for the employee medical file, but not specific to the audio information collected.

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

Privacy Risk: Contractor may not know an employee has left federal/civilian employment, or a different contractor may be used in the future.

Mitigation: A new contractor will utilize the same server created by OCIO and no gap in service will occur whenever a new contractor starts.

The Contractor Officer Representative (COR) receives (from Human Resources) Accessions and Separation Reports on a monthly basis. The COR uses the report to notify the contractor of New Hires and identify employees who have transitioned from the agency. Employees who have separated from the agency will be subsequently identified in the contractor's system as "Inactive."

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 information collected is only shared with Human Resource Department for upload to the employee medical file.

FSIS will collaborate with the vendor to establish the previously mentioned secure file server that adheres to robust encryption protocols and incorporates identity and access management controls such as Login.gov. This server will facilitate the secure exchange of data between the vendor supporting HCP for FSIS employees, and the FSIS HR staff who require access.

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

Privacy Risk: Low risk that information transmittal in the Human Resources Department inadvertently releases PII.

Potential for a privacy incident when information is transferred from the contractor to FSIS secure server.

Mitigation: Follow department policy regarding incident response and reporting of privacy incidents.

The contract will specify damages for privacy incidents and contain provisions for liquidated damages.

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?

FSIS will share and receive information from the contractor.

The shared/received/transmitted information is the audiometric testing results and the necessary PII for the testing process.

The secure file server will be used for the transfer of data between the contractor and FSIS.[9]

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

Privacy Risk: Inadequate security controls such as weak encryption, or a lack of access controls could lead to an incident or breach.

[9] The secure file server will adhere to robust encryption protocols and incorporates identity and access management controls such as Login.gov. This server will facilitate the secure exchange of data between the vendor supporting HCP for FSIS employees, and the FSIS HR staff who require access.

Mitigation: The secure file server will adhere to robust encryption protocols and incorporate identity and access management controls such as Login.gov. The server will facilitate the secure exchange of data between the vendor supporting HCP for FSIS employees, and the FSIS HR staff who require access.[10]

The vendor system must have a FedRamp certification to ensure adequate security controls are in place to safeguard the confidentiality, integrity, and availability of the HIPAA data.

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?

Participants will review their information on the Portable Audiometric Testing Device prior to the test. The portable audiometric device will also contain information on contacting Human Resources in the event an inaccuracy is discovered.

Employees may also obtain a copy of their records by sending a request via email to HR (Medical Records Administration Specialists). The HR Specialist will verify the requester and send encrypted records to the requesting employee's work email.

Participants can additionally contact Food Safety and Inspection Service (FSIS) Human Resources: 1-877-374-7471 to reach FSIS HR representatives Monday-Friday from 8:00 a.m. to 4:00 p.m. Participants may also mail FSISH1@usda.gov.

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

Prior to the start of the examination, the employee must verify/check the information on the Portable Audiometric Testing Device for accuracy. Participant employees will additionally be responsible for input of some personally identifiable information (such as age and gender) on the device.

[10] The collected information is safeguarded by leveraging the Transport Layer Security 2.X (TLS 2.X) encryption across the communication medium between the vendor and location point where the data resides. The disk storage area is encrypted for data at rest, which protects confidentiality. Additionally, an in-line web application firewall proxy service is in place restricting malicious activity (i.e. Distributed Denial of Service attacks, BOT attacks, and Orchestration attacks).

The device will contain notice regarding who to contact in HR if information needs correction.

Additionally, participants can contact Food Safety and Inspection Service (FSIS) Human Resources: 1-877-374-7471 to reach FSIS HR representatives Monday-Friday from 8:00 a.m. to 4:00 p.m. Participants may also mail FSISH1@usda.gov.

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

The portable audiometric device will contain notice regarding who to contact in HR if information needs correction.

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

Formal redress is provided, and FSIS personnel may contact Human Resources directly for assistance.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: Failure of the redress process may cause an employee to not understand how errors can be corrected.

Mitigation: The device will contain notice regarding who to contact in HR if information needs correction.

Participants can also contact Food Safety and Inspection Service (FSIS) Human Resources: 1-877-374-7471 to reach FSIS HR representatives Monday-Friday from 8:00 a.m. to 4:00 p.m. Participants may also mail FSISH1@usda.gov.

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?

The vendor/contractor selection includes requirements that their cloud system be FedRamp compliant since they are providing the services to store HIPAA data in their cloud system. FedRamp ensures that vendors providing services to the government have an approved set of controls in place to secure PII.

FSIS will establish a secure server that adheres to robust encryption protocols and incorporates identity and access management controls through multifactor identification. This server will facilitate the secure exchange of data between the vendor supporting HCP for FSIS employees, and the FSIS HR staff who require access.

Additionally, FSIS will require the contractor sign a Non-disclosure Agreement (NDA).

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

The COR has sole access to the secure file server. The contractor will identify personnel with access to the server.

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

All users are required to annually complete the Security and Awareness training program on Ag Learn. All vendor users will be trained in and meet HIAPA privacy and security requirements.

Approval Signatures:

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

Marvin Lykes
CISO/ACISO
Food Safety Inspection Service
United States Department of Agriculture

DAVID LINDNER
Digitally signed by DAVID LINDNER
Date: 2024.03.21 09:43:44 -04'00'

David Lindner
Chief Privacy Officer
United States Department of Agriculture